NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SHORT-TERM CYBER-ATTACKS WITH LONG-TERM EFFECTS AND DEGRADATION OF SUPPLY CHAIN CAPABILITY

by

Jose M. Lamberty

September 2016

Thesis Advisor:	Gary O. Langford

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704–0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2016	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE SHORT-TERM CYBER-ATTACKS WITH LONG-TERM EFFECTS AND DEGRADATION OF SUPPLY CHAIN CAPABILITY	**5. FUNDING NUMBERS**
6. AUTHOR(S) Jose M. Lamberty	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Historically, cyber-attacks targeting computer networks have sometimes favored the attacker over the defender, resulting in great loss of information or denial of service. This thesis investigates the possibility that short-term cyber-attacks on network supply chains may conceal more sinister plans to destroy the long-term operational effectiveness for supplying goods during periods of critical needs. Using a life-cycle approach, quantifiable metrics were used to compare short-term risks with long-term risks in a network supply chain to establish the existence of black swan events.

14. SUBJECT TERMS cybersecurity, supply chain risk management, vulnerabilty analysis, short-term, long-term, black swan, quantifiable supply chain metrics	**15. NUMBER OF PAGES** 85
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

SHORT-TERM CYBER-ATTACKS WITH LONG-TERM EFFECTS AND DEGRADATION OF SUPPLY CHAIN CAPABILITY

Jose M. Lamberty
Lieutenant Commander, United States Navy
B.S., Jacksonville University, 2002
M.S., Naval Postgradute School, 2008

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2016

Approved by: Gary O. Langford
Thesis Advisor

Ronald Giachetti
Chair, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Historically, cyber-attacks targeting computer networks have sometimes favored the attacker over the defender, resulting in great loss of information or denial of service. This thesis investigates the possibility that short-term cyber-attacks on network supply chains may conceal more sinister plans to destroy the long-term operational effectiveness for supplying goods during periods of critical needs. Using a life-cycle approach, quantifiable metrics were used to compare short-term risks with long-term risks in a network supply chain to establish the existence of black swan events.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ASD(L&MR)	Assistant Secretary of Defense for Logistics & Materiel Readiness
DASD(SE)	Deputy Assistant Secretary of Defense for Systems Engineering
DOD	Department of Defense
IP	Internet Protocol
ISO	International Organization for Standardization
JFAC	Joint Federated Assurance Center
NIST	National Institute of Standards and Technology
TCP	Transmission Control Protocol
U.S.	United States
US-CERT	United States Computer Emergency Readiness Team

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Historically, cyber-attacks on computer networks have favored the attacker (Red) over the defender (Blue), often resulting in loss of data and compromising the Blue's ability to maintain control of its network operations. Detecting malicious software in monitored, secure environments has proved quite challenging, generally lagging the discovery of consequences of the cyber-attack(s) (e.g., data that was stolen). Although computer network operators (Blue) have been very aggressive in responding to cyber-attacks once the consequences have been observed, the short-term response of the network defenders has focused on a quick response with security updates to prevent that attack from happening in the future. Blue's objective is to return the network to fully functioning operations by regaining explicit, non-compromised "control" of the network for Blue.

This thesis poses the possibility that Red's short-term cyber-attacks may be harbingers of more sinister plans to destroy the operational effectiveness of network operations, (i.e., a supply chain planned to meet critical operational needs of commercial or military operations). In this regard, some of Blue's best practices against cyber-attacks may have the intended effect of allaying short-term anxieties, yet pose grave risks for unexpected events on a long-term basis. This thesis answers the important question: how can short-term responsiveness to cyber-attacks on supply chains boost long-term dangers of black swan events meant to destroy supply chain effectiveness for a critical period? The investigation adopts a life-cycle approach to analyze the functions and processes within a network supply chain to determine the changes in management metrics for short-term and long-term risks. We analyze long-term risks in terms of black swan events to determine their origins in short-term cyber-attacks. As proposed by Nickolas Taleb (2010), black swan events are those that although improbable—with a probability of occurrence of less than 5%—once they occur their effects can be catastrophic. These events are labeled as improbable because current statistical models have them fall greater than four standard deviations outside the normal distribution. Hence, these events are considered as outliers and are therefore ignored in all standard risk assessments.

The supply chain is defined as “physical and logical flow of goods, information, processes, and money, upstream and downstream through a supply chain. They may include supply chain nodes, locations, delivery paths, or transactions,” (NIST 800–161 2015, F6). Supply chain management has long been involved in the management of acquisitions, support, and logistics for goods and services. The evolution of the supply chain now extends to distribution networks, information management, customer support, and logistical activities. Cybersecurity issues in the supply chain have compelled government and commercial entities to allocate significant time and money to attempt to cope with the potential of mission degradation caused by the susceptibility of the supply chain to threats and the vulnerable supply chain processes. Most of the “fixes” implemented by commercial and governmental entities are short term.

Short-term responses by Blue to a cyber-attack are defined in this thesis as those involving an immediate response to thwart or observe, and corrective action to ameliorate a newfound vulnerability. Long-term views and strategies of Blue are those that over time may pose catastrophic effects when not addressed adequately in the short-term when there is time to correct structural problems in architecture and assess the vulnerabilities and susceptibilities. A short-term cyber-attack that has long-term vulnerability potential with catastrophic consequences was the attack on the U.S. Office of Personnel Management (OPM) (Committee on Oversight and Government Reform 2015). Stuxnet is another example of how a short-term attack can have long-term implications. Stuxnet is known as an attack to a government infrastructure with the intent to degrade (long-term effect) the capability of Iran to enrich weapon-grade uranium (Kushner 2013).

Under the assumption that Red’s intent is to introduce some sort of stressor or stimulus with the ultimate goal of gaining insight of an organization’s internal process that generate a particular observable. Blue is resource constrained while Red’s attacks are numerous with unlimited resources. Red may be not be looking for a specific observable but rather just looking for what are the observables generated by the attack. The model is represented graphically in Figure A. In the short-term model, Blue does not recognize the long-term implications or relationship between attacks.

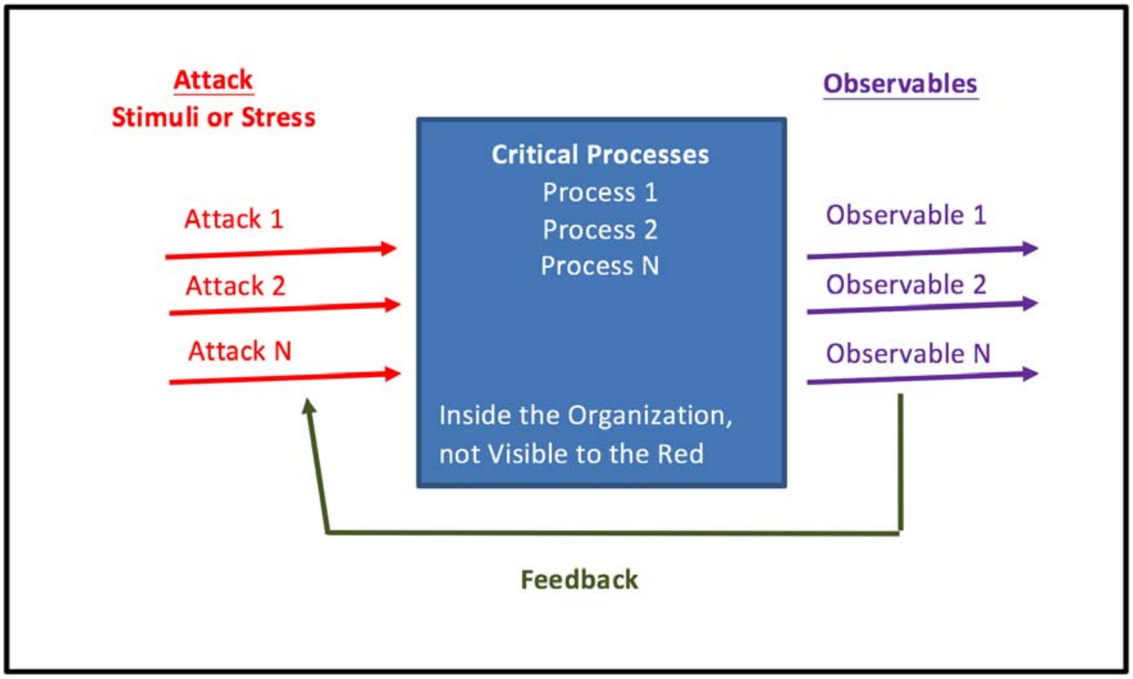


Figure A. Illustration of the Multitude of Attacks and Observables to Take into Account in the Supply Chain.

Orlik and Veldkamp define a black swan event as one that exhibits uncertainty fluctuations caused by "time-varying risk of unobserved tail events" (2015, 2), in other words a "conditional probability of a rare event" (2015, 4). These "tailed" events relate to the thickness of the expected distribution tails, also known as skewness. Such fluctuations assume that the true distribution of supply chain vulnerabilities occur as unknowns. The significant contribution of Orlik and Veldkamp was to explain large fluctuations in uncertainty due to changes in the likelihood of events that were distributed far from the mean of the data (2015). Through a careful analysis of the causes of statistical significance, it was not the changes in the variance in the data that was the culprit but rather the time-varying risk of the unobserved tail events, which are also known as black swans. "Thus, everyday fluctuations in a data series can produce large fluctuations in conditional variance for an agent who is constantly re-estimating the tails of the distribution" (Orlik and Veldkamp 2015, 1).

For long-term objectives, Red will generate one attack (Attack 1) on the system that eventually causes Blue to respond and cause an external observable (Observable 1).

Observable 1 is monitored and fed back (Feedback 1) to Red. Red in turn generates subsequent attacks (in a series, parallel, single, or simultaneous) denoted as Attack N, which generates an Observable N, and fed back N number of times. The process continues where Blue may not notice the interrelation between the attacks. At a future time, Red decides to initiate all or a series of attacks to attain an effect (black swan) to case mission degradation. Notice the difference in the feedback loop in the long-term versus short-term objectives. For long-term objectives, the feedback provides the initial conditions for the next attack. The short-term objective feedback provides an observable for Red, and it ends there. From Blue's perspective, the multiple attacks may not be related. The long-term model is represented graphically in Figure B.

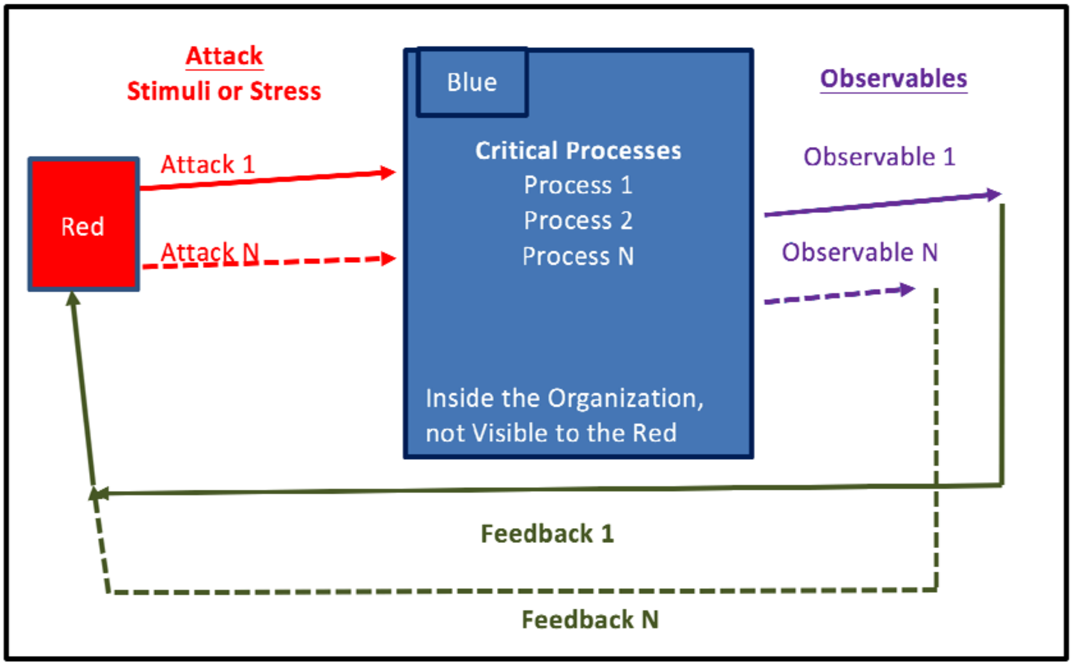


Figure B. Long-term Model Illustration of the Multitude of Attacks and Observables on the Supply Chain.

From the supply chain's short-term and long-term perspective, once Blue determines that a problem is detected in the type of goods that are planned to be transited to a location with an urgent need and has determined mitigating measures for all identified risks, then the likelihood and consequence can be recorded in risk register for traceability of risks and their associated ratings (DASD[SE] 2015).

Long-term views must consider the short-term metrics and how a combination of those metrics may provide the big picture of what will be the black swan event (Red's long-term objective). Blue must use the tools and metrics provided in this thesis together with external process (e.g., organizational audits, health assessments) to attempt to identify those long-term black swan events. The idealization of a supply chain black swan caused by Red, posed as the premise of this thesis, substantiates the notion that short-term cyber-attacks can indeed be considered as precursors for long-term problems.

References

House of Representatives Committee on Oversight and Government Reform. 2015. *OPM: Data Breach.* House of Representatives, Washington, DC, Rayburn House Office Building.

Kushner, David. 2013. "The Real Story of Stuxnet." Institute of Electrical and Electronics Engineers. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

Office of the Deputy Assistant Secretary of Defense for Systems Engineering. 2015. *Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs*. Washington, DC: Office of the Deputy Assistant Secretary of Defense for Systems Engineering, June 1. http://www.acq.osd.mil/se/docs/RIO-Guide-Jun2015.pdf

Orlik, Anna, and Laura Veldkamp. 2015. "Understanding Uncertainty Shocks and the Role of Black Swans." Working paper, National Bureau of Economic Research.

National Institute of Standards and Technology. 2015. *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*. NIST SP 800–161. Gaithersburg, MD: National Institute of Standards and Technology.

Taleb, Nicholas. 2010. *The Black Swan: Second Edition: The Impact of the Highly Improbable*. New York: Random House.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

To my wife and kids, thanks for your ongoing support throughout all of our personal and professional milestones.

Dr. Langford, thanks for your ongoing support and mentoring. Without your guidance during this process, this accomplishment would have not been possible.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Systems engineering spans the life-cycle of products and services, encompassing conceptualization, development, integration, operations, sustainment, and disposal. Once a service has been placed into operations, goods are moved through a chain that supplies and provides services to customers. This supply chain is defined as "physical and logical flow of goods, information, processes, and money, upstream and downstream through a supply chain. They may include supply chain nodes, locations, delivery paths, or transactions," (NIST 800–161 2015, F6). Since the introduction to supply management by Frederick Taylor in 1911 (Taylor 1911), supply chain management has long been involved in the management of acquisitions, support, and logistics for goods and services. The evolution of the supply chain now extends to distribution networks, information management, customer support and logistical activities. Supply chain management has developed into its own field, now addressing vulnerabilities to physical and cyber-attacks in the private, commercial, and government sectors (Warren et al. 1990; Shackleford 2015).

Defining military and commercial readiness in terms of available resources to operate in both normal and unforeseen situations challenges the means of providing defense-critical goods and services through a network of suppliers. To underscore the need for a robust and resilient supply chain in spite of the complexities of supply chain management, the susceptibilities and vulnerabilities of supply chains, coupled with the added complexities of cybersecurity, poses new challenges to readiness. Cybersecurity concerns are prominent, as shown in Internet and news media headlines of companies (i.e., Target Inc., Home Depot, and the Office of Personnel Management (OPM)). In hundreds of examples, "secure" networks were hacked and sensitive information was compromised and stolen to gain access to economic, military, and private data (Krebs 2014). For the United States (U.S.) Department of Defense (DOD), cybersecurity is defined as the "prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation" (DOD 2014a, 55). When cybersecurity is inadequately implemented, the short-term implications can be catastrophic—from loss of customer privacy data to mission failure due to degradation of capability and effectiveness of the supply chain.

Security against cyber threats has grown to become a top concern for the military, government officials, corporations, and individuals. In an effort to address the multitude of cybersecurity incidents that have weakened the country's critical infrastructure, President Barack Obama signed Executive Order No. 13636 in February 2013. This order directed the increase of shared cybersecurity information with the private sector, accomplished by declassifying federal cybersecurity reports and making them available for private use. The rationale provided in the order was that the private sector would be better protected and able to defend itself against cyber threats by bringing forward voluntary information. This voluntary information should consist of cyber related institutional lessons learned, assessments and implementation of corrective actions, which the goal of providing transparency. The Executive Order tasked the Department of Commerce's National Institute of Standards and Technology (NIST) with developing the mechanism to consolidate inputs from organizations, inside and outside the government, to develop standards and best practices for improving the infrastructure. Other issues addressed in Executive Order 13636 include safeguarding privacy, auditing current cybersecurity doctrine, and encouraging the private sector to join the framework created by NIST (2013). Further, The National Defense Authorization Act (2013) for Fiscal Year 2014, §937, called for the establishment of a "joint federation of capabilities" to ensure security of DOD software and hardware. In response to the 2013 act, United States Deputy Secretary of Defense (2015) Robert Work signed Policy Memorandum 15–001, which authorized the creation of the Joint Federated Assurance Center (JFAC). The Deputy Secretary of Defense (2015) stated that the JFAC would be implemented by the Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics (DASD[SE]). The Undersecretary of Defense described the purpose of the JFAC as providing support to program offices through their acquisition life-cycles to implement future policies as well as software and hardware expertise in the form of standards, requirements, best practices, contracting, training, and testing (DASD[SE] 2015). On February 9, 2015, Deputy Secretary of Defense Robert O. Work signed the charter for a new organization (Hurt 2015). At the time of publication, the official JFAC website was not available.

To underscore the similarities between commercial and military supply chain issues, problems, and management, Dr. Kristine Leiphart from Rand Corporation, writing for the Army Logistics University, reiterated that, "Military logistics and commercial logistics are parts of the same industry" (Leiphart 2001). The national infrastructure networks that support supply chains for both military and commercial uses may be stressed at some point, so that the military supplies might jointly use public assets or in critical circumstances take priority over supply of commercial goods. The same concerns to reduce inventory, use technology to improve efficiency, outsource to certain vendors, use commercial rates for some military supplies, and to thwart cyber-attacks on the commercial supply chain infrastructure are akin to deterring cyber-attacks on the military supply chains.

Cybersecurity issues in the supply chain have compelled government and commercial entities to allocate significant time and money to attempt to cope with the potential of mission degradation caused by the susceptibility of the supply chain to threats and the vulnerable of the supply chain processes. Most of the "fixes" implemented by commercial and governmental entities are short term—to sustain the movement of goods to maintain the utility of the supply chain. Long-term effects are presumed to be accommodate by the current best practices of supply chain management (i.e., concerned with focused logistics, precision and velocity, coordinated delivery schedules, fast and flexible distribution, and good infrastructure and equipment at distribution centers (Leiphart 2001). Appendix A contains DOD and commercial short-term vulnerability management frameworks and initiatives.

A. PURPOSE OF THESIS

The purpose of this research is to develop a framework of thinking about cybersecurity in both the short term for responding to immediate problems and in the long term to treat the short-term problems as a means to structure cyber-attacks that may disrupt or incapacitate the flow of goods.

B. PROBLEM

Successful cyber-attacks are inherently disruptive. The means of disruption can range from extracting data and information about what is moving through the supply chain, how the movement of goods is managed, and to include shutting down complete operations. The efforts to maintain cybersecurity are seemingly frustrated by legacy systems that are incompatible with modern technology, inadequate recognition of the sophistication of the cyber threats, and detection of the most insidious threats that are quiescent until activated later. Continuing to deal with cyber-attacks as short-term "inconveniences" that disrupt "smooth" operations in a supply chain, may prove insufficient for long-term supply chain effectiveness. Without effective movement of goods through supply chains, customers and users of these goods may find themselves without access to those goods during periods of critical operational requirements. Both commercial and military supply chains may fail when they are most needed. The problem is without the required goods from supply chains organizations may fail to accomplish strategic or mission objectives, resulting in catastrophic losses.

C. RESEARCH QUESTION

How can short-term responsiveness to cyber-attacks on supply chains boost long-term dangers of black swan events? A short-term metric that is monitored for missing items in a shipment to a particular location may be interpreted as a need to resend the missing items to that location. The cause and effect are assumed to be that an item was missed when loading the vehicle for transit. However, if the result of a cyber-attack was intentionally to deceive the management of the flow of goods in the supply chain, then the cause may have been to ship the missing item intentionally to another location and then gauge the response of the network control. If the network control responded by simply rerouting the “missing” item to its “proper” location, then the cyber-attack may have established a long-term means of shipping all items to wrong locations and therefore all parts will be “missing.”

D. APPROACH

The investigation adopts a life-cycle approach from systems engineering to analyze a network supply chain in terms of its processes and functions. Functions are quantifiable and therefore can be cast into management metrics to help identify short-term and long-term risks. These metrics are developed to analyze long-term risks in terms of black swan events to determine their origins in short-term cyber-attacks. As proposed by Nickolas Taleb (2010), black swan events are those that although improbable, with a probability of occurrence of less than 5%, once they occur their effects can be catastrophic. These events are labeled as improbable because current statistical models have them fall greater than four standard deviations outside the normal distribution. Hence these events are considered as outliers and are therefore ignored in all standard risk assessments.

This study addresses the methodology needed to harden the supply chain to mitigate the vulnerabilities associated with the cybersecurity supply chain. This was accomplished by studying and gaining an understanding of the top-level overarching Executive Order 13636 (2013), the subsequent documents that have supported it, and by understanding cyber-attackers’ short-term and long-term objectives.

The purpose of Chapter II is to establish a baseline to identify the processes in a generic supply chain. This was accomplished by introducing the concept of conventional supply chains, their importance and by defining supply chain functional and behavioral boundaries. With the ultimate goal of determining functional performances and their quality attributes, as well as defining a supply chain as a network of things. Current DOD and commercial industry efforts regarding cyber-supply risk as well as their applicability to cybersecurity are presented, together with frameworks and initiatives for supply chain vulnerability management. In addition, Chapter II contains the DOD's promulgated supply chain vulnerabilities and explains what makes them so unique as well as why current methodology may not address the cyber threat. All of these efforts and initiatives were leveraged to better understand the problem.

After compiling the material for Chapter II, it became clear that issues in the current supply chain methodology revolved around short-term techniques that subjectively enumerate, rank, and then assign impacts and consequences. In addition, most mitigation strategies focused on short-term solutions. Chapter III introduces the concept of black swan theory as it applies to long-term effects and the proposed long-term model and the nature of hardening supply chains by applying the long-term model.

E. LIMITATIONS AND ASSUMPTIONS

This study was conducted from the supply chain perspective. Although cybersecurity is discussed in this thesis, the intent is not to dwell on the technological details associated with cyber-attacks, but rather provide a holistic approach to harden the supply chain in the short term and long term. Due to the proprietary nature of cybersecurity risk management and lack of publicly available data, the literature review was conducted from officially released public sources using both private sector and government documents.

Specific stakeholders were inferred from federal and private sector instructions and regulations. These stakeholders include government and private sector organizations that are susceptible to supply chain cybersecurity threats.

For the purposes of this thesis, supply chain vulnerability is that which can lead to business risk. The Blue perspective (Blue) is defined as the organization or industry trying to harden its supply chain from cyber-attacks. The Red perspective (Red) is the attacker, trying to gain access to the system to control or gain valuable information. From Blue, the agent is operating from the inside looking out. Red is trying to gain access to Blue's resources from the outside looking in. Blue and Red are analyzed from the perspectives of short-term and long-term views. The short-term and long-term views are nothing less than short-term and long-term objectives.

F. SHORT-TERM AND LONG-TERM VIEWS

Blue vulnerability to Red cyber-attacks can have short-term or long-term consequences. Short-term vulnerabilities (e.g., tampering, theft, unauthorized production, counterfeits, poor manufacturing (NIST 800–161)), come with consequences that can be remediated and goods flow with most likely only a few encumbrances. Long-term vulnerabilities include reduction of the ability to complete overall mission (e.g., loss of ships in a squadron, manufacturing and or delivery of parts for weeks and months at a time), with consequences that will perhaps require substantial rework, reorganization, and changes in infrastructure. Regardless of the terminology of short term or long term, supply chains can be damaged sufficiently by cyber-attacks so that they become useless in critical situations (i.e., when the supplies are needed to avoid harm because of lack of goods). Blue supply chain managers need to assess short-term vulnerabilities to determine if there are also long-term consequences that may aggregate to disrupt the supply chain over a longer period. Further, cyber-attacks may appear to be of a particular nature that has a short-term fix, while in fact the cyber-attack might also be geared to set the stage for a more insidious attack that completely disrupts the supply chain during an urgent and very critical situation. The short-term remediation may portend long-term problems for Blue that could arise on a future date certain or be triggered by another seemingly short-term cyber- or physical attack that cause overall mission failure.

An example of a short-term cyber-attack that opens up a potential long-term vulnerability with catastrophic consequences is the attack on the U.S. Office of Personnel Management (OPM) (Committee on Oversight and Government Reform 2015). More than 22.1 million current and former federal employees (Naylor 2015) data on Standard Form 86 (https://www.opm.gov/forms/standard-forms/) was exfiltrated—meaning that the data was removed from the network by the adversary who took it (Committee on Oversight and Government Reform 2015). In addition, data on the contractors and suppliers for the DOD on Standard Form 18 were also disclosed in a separate cyber-attack (Committee on Oversight and Government Reform 2015). The same group of Chinese hackers associated with the Chinese Red Army was implicated in all of these cyber-attacks and data were exfiltrated by the same Chinese hackers associated with the Chinese Red Army (Committee on Oversight and Government Reform 2015). The short-term response is for Blue to shore up cybersecurity by upgrading servers, applying new security measures to restrict access, and to put in place more sophisticated software to determine if a breach has occurred. The data breaches of these federal data bases lasted upwards of 150 to 200 days (Committee on Oversight and Government Reform 2015). Red first penetrated the security systems of the contractors with cyber-attacks that provided inputs to the OPM, and then used their knowledge to exfiltrate information on people and suppliers in the DOD supply chains. The long-term vulnerability may be from malicious software code that remains on the data servers until activated (later). Imagine integrating data for suppliers involving movements of DOD personnel in a massive assessment of supply chain readiness to deliver goods, assessment of capability to deliver goods, and responsiveness to cyber-attack. By potentially malicious management through a Red cyber-attack, the movement of goods in proper numbers to proper destinations could be coopted. The supply chain would initially appear to be operating as normal, but when the wrong shipments begin to arrive at their unintended destinations, the extent of the damage will be realized by Blue. Valuable time will have been lost for Blue, and Red may have perpetrated a massive disruption of a vitally needed military supply effort. By its nature, the short-term view necessarily must focus on the immediate shipment of good, whereas, the long-term view requires a broader look at the totality of possible consequences. The long-term view of Blue is necessarily a systems view where methods and tools of systems engineering lend themselves to supply chain planning, analysis, and sustainment (Childerhouse 2011; Tsai 2011; Pistikopoulos et al. 2011).

Short-term responses by Blue to a cyber-attack are defined in this thesis as those involving an immediate response to thwart or observe, and corrective action to ameliorate a newfound vulnerability. A typical short-term view of Blue is one that normally involves widely used risk management tools and techniques (quantitatively and qualitatively) and mitigation strategies. Short-term fixes that control the physical movement of goods normally involve software and or hardware patches, firing underperforming suppliers, repairing failed manufacturing equipment, rerouting delayed packets, assigning an alternate platform in lieu of damaged or platforms under repair. Red's goal could be to gain control of a computer(s) that controls or leads to control of Blue's supply chain(s). For short-term objectives, Red may want to degrade the supply chain so that Blue would need to spend more time and money but without Blue being able to identify Red. Short-term attacks that are left unchecked by Blue can lead to mission failure. Such is the case with Stuxnet.

Stuxnet is a highly recognized and known attack to a government infrastructure with the intent to degrade the capability of Iran to enrich weapon's grade uranium (Kushner 2013). The computer worm of 500 kilobytes software code, with the capability of replicating itself, was installed in the control system that managed the centrifuge farm (Kushner 2013). According to Kushner, the worm targeted the plant's computers operating system to multiply and reach across multiple computers, infected the software used to operate the plants equipment, and then controlled the digital computers used for plant's automation to increase the speed to the centrifuges just enough to increase their maintenance, removal, and replacement. The Stuxnet worm did not require an intranet connection, something as simple as a portable drive could be used as the insertion device into the system spreading the worm to other computers via the intranet without user intervention. Further, the Stuxnet worm sent confusing signals to other computers in the system so that its masquerade could continue by using digital certificates to trick the operating system into accepting its executions as a legitimate program from a trusted source. The result was catastrophic failure with reduced capability and effectiveness.

In the military case, Red's objectives could be to obtain and modify information about accessing the supply chain's management processes for sort term and long-term processes. Short-term disruptions of Blue could also be considered to be information gathering to facilitate Red's long-term objectives (i.e., to prepare long-term strategies for catastrophic failure of Blue's supply chain).

Long-term views and strategies of Blue are those that over time may pose catastrophic effects when not addressed adequately in the short-term. The intention is for Blue to take advantage of the short-term knowledge when there is time to correct structural problems in architecture, assess the vulnerabilities and susceptibilities. That also leaves Blue time to evaluate the alternative strategies and means of protecting data and information. Datum is a quantity or quality that is measured, assigned, or computed. Information is the correspondence between datum and context. The Red long-term view is to cause Blue to have catastrophic mission failure(s), whereas the Red short-term view may be simply to degrade.

II. SUPPLY CHAIN MANAGEMENT, VULNERABILITY, AND RISK

Managing the flow of goods in anticipation of cyber-attacks on a short-term basis requires specific attention to the network of stakeholders in the supply chain, their assurance policy and procedures for protecting both information essential to supply chain security and for accessing the controls, planning, architecture, communications, commands, and stakeholder intentions. Prohibiting, responding, or observing cyber-attacks are the responsibilities of supply chain management.

The Council of Supply Chain Management Professionals (2013), the leading industry association that sets standards and provides professional training and accreditation, defines supply chain management as follows:

> The planning and management of all activities involved in sourcing and procurement, conversion, and all logistics management activities. Importantly, it also includes coordination and collaboration with channel partners, which can be suppliers, intermediaries, third-party service providers, and customers. In essence, supply chain management integrates supply and demand management within and across companies. Supply Chain Management is an integrating function with primary responsibility for linking major business functions and business processes within and across companies into a cohesive and high-performing business model. It includes all of the logistics management activities noted above, as well as manufacturing operations, and it drives coordination of processes and activities with and across marketing, sales, product design, finance and information technology. (187)

This definition implies that the important aspect of managing the supply chain is mainly driven by supply and demand. One aspect that the council does not define is how the quality of produced items or processes are assessed to certify they have not been compromised.

Zsidisin and Ritchie (2008) define supply chain vulnerability management as the implementation of strategies to manage vulnerability along the supply chain. They argue that vulnerabilities can be mitigated with continuous monitoring, assessment, and effective corrective actions, with the ultimate objective of reducing vulnerability and ensuring continuity in the supply chain. When comparing the definitions of supply chain management by Zsidisin and Ritchie (2008) and the Council of Supply Chain Management Professionals (2013), Zsidisin and Ritchie's definition seems better suited to the needs and requirements of the cyber supply chain because it addresses mitigation of vulnerabilities through continuous monitoring and assessment.

The definition from Council of Supply Chain Management Professionals implies that supply chain management is reactive to changes in supply and demand. Today, due to the complexities involved with purchasing, warehousing, controlling stock, and emerging cyber threats, the supply chain has evolved, and the analysis of its vulnerability requires a more rigorous approach.

A. CONVENTIONAL SUPPLY CHAIN

The typical supply chain used for commercial and military activities is comprised of multiple process flows: information, goods, packaging material, transportation, and funds (Scott et al. 2011). The supply chain is normally driven by either product supply or customer demand. Supplying the product before or just when the customer needs the product (i.e., product supply) is typical of routine customer demand, sometimes accelerated by nominal changes in need (Scott et al. 2011). The product supply approach presumes there is both an insufficiency of storage space at the delivery site and that the customer demand is matched with the production and customization, if any. In other words, the supply chain that supplies products before the customer has the actual need, helps moderate the amount of money tied up in goods in transit that cannot be sold or used and obviates the need for inventory storage beyond what needs to be accommodated to match with sales or use. In contrast, a supply chain that is customer driven may need to have been customized or some form of modification to satisfy details needed by the customer (Scott et al. 2011). Figure 1 shows a basic supply chain with flows of information (customer's order), funds (customer's payment), and the supplier's product delivery. In this particular figure, the product is tea or coffee.

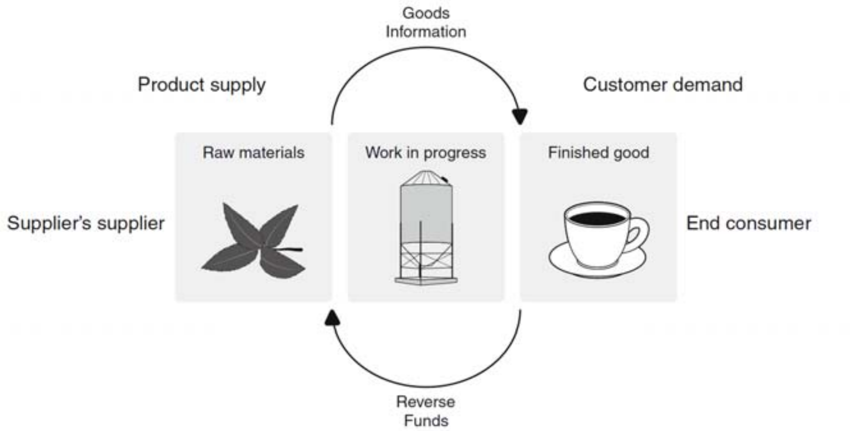


Figure 1. The Simplified Supply Chain for Tea or Coffee. Source: Scott et al. (2011).

Once the order is received from the customer or generated internally by the source, (i.e., the entity that supplies the good, the source makes the decision to make—build to stock; make—build to order; make—engineer to order; buy to stock; have built to stock; or have engineered to stock). The "make" decisions are premised on having all components, whereas the "buy," "have built," and "have engineered" decisions are necessary when source supplier does not have the necessary components in stock.

In the short-term view, management of the flow of goods is paramount—ensuring production and distribution satisfies demand. Cyber-attacks can gather information by which to harass, embarrass, or disrupt. All such acts can take substantial resources to counter, and if the long-term view is not reflected in the assessment and evaluation of Red's intentions, then management will tend to focus on exactly making and moving goods to placate customers and users.

B. SUPPLY CHAIN'S FUNCTIONAL AND PROCESS DESCRIPTION

According to the Supply Chain Council the functional aspects of the supply chain are modeled in the Supply Chain Operations Reference (SCOR) model (Scott et al. 2011). As depicted in SCOR, the functions of the supply chain are very broad and complex and illustrated in Figure 2. The SCOR model functional aspects are divided into plan, source, make, deliver and logistics (or returned products). All of the processes are repetitive and occur during all stages of the supply chain.

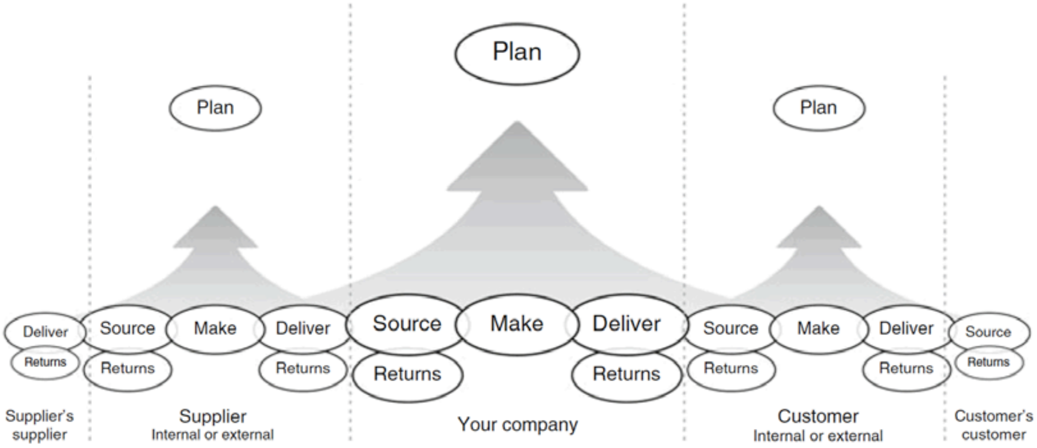


Figure 2. Supply Chain Operations Reference Functional Aspects of the Supply Chain. Source: Supply Chain Council (APICS) (2016).

The first stage in SCOR is planning (Scott et al. 2011). Based on supply and demand triggers, a plan is developed to accommodate the limitations on the availability of source good, source production issues, and delivery constraints affecting all entities in the chain of processes that move goods. The next stage is to find the right suppliers (purchasing or procurement) based on the needs of customers, users, and source. After planning and souring is complete, the manufacturing or tailoring of the product commences. Once the product is manufactured, it can be delivered. Delivery includes warehousing and transportation of goods. Then, the goods are inspected and accepted. The final steps in the supply chain are to return products from the customer due to unacceptable quality, recycling, or repair.

The customer–contractor relationship requires flows of information and services. The service, product delivery, is the focus of this thesis. The stakeholders in the supply chain are the customer (Blue), who is in need of a product for the user, the provider of raw materials to the contractor and or subcontractor, and the transporter used to transport all raw and finished material. These relationships are illustrated in Figure 3. The flows of information and deliveries are denoted by dotted lines and arrows, respectively. The Source of Raw Materials communicates (dotted lines) with the Transporter and the Contractor, while it uses the Transporter to deliver (arrows) the product. The Contractor communicates (dotted lines) with all Subcontractors, Transporters, User and Customer. The Contractor uses the flow of information to accept deliveries from Subcontractors and deliver to the User, at the Customer's request. The Customer is the liaison between the User (requirements and services) with the Contractor. The User uses the Transporter to receive delivery or to return products to the Contractor. The User communicates with the Transporter, Customer and the Contractor. The flow of information and services within the supply chain manages the actions of the supply chain. Control of that information determines the effectiveness of the movement of goods. The vast majority of supply chains are computer controlled and those computers are vulnerable to cyber-attack.

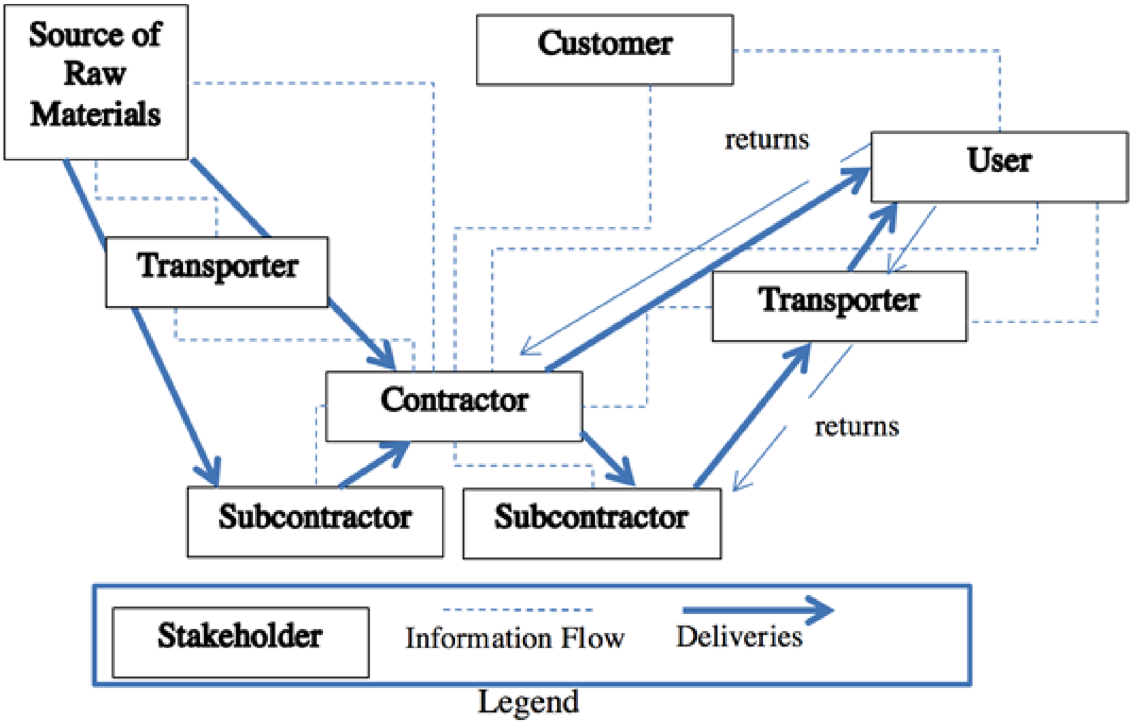


Figure 3. The Flow of Information and Services within the Supply Chain.

For both short-term and long-term thinking, the process decomposition expands the SCOR to include processes related to cybersecurity issues.

Of particular importance to this research are the implications of a catastrophic failure of the supply chain. As proposed by Nickolas Taleb (2010), black swan events are those that although improbable, with a probability of occurrence of less than 5%, once they occur their effects can be catastrophic. These events are labeled as improbable because current statistical models have them fall greater than four standard deviations outside the normal distribution. Hence, these events are considered as outliers and are ignored in all standard risk assessments. These outliers are considered black swans.

Taleb continues by explaining that most currently used models rely on relationships and degrees of uncertainty that may only be effective for short-term forecasting, but fall short when trying to explain real word events (2010). These models are synonymous to inside the box thinking, where all dynamic aspects of the events in question are not considered. The black swan perspective can be applied to long-term supply chain vulnerability. A long-term black swan vulnerability, when it occurs, can destroy supply chain operations.

These high-level processes are:

1.1 “to forecast”
    1.1.1 “receive demand signals”
    1.1.2 “interpret customer demand signals”
    1.1.3 “assess response to demand signals”
    1.1.4 “evaluate responses to demand signals”
1.2 “to plan”
    1.2.1 “determine the problem”
    1.2.2 “evaluate options for responding to demand signals”
        1.2.2.1 “provide for steady state delivery (with nominal variance)”
        1.2.2.2 “provide for steady state delivery (with surge variance)”
        1.2.2.3 “provide for emergency delivery”
    1.2.3 “identify the risks”
1.3 “plan reverse logistics”
    1.3.1 “adjust design/architecture”
    1.3.2 “adjust execution/control”

1.4 "to determine risk (combination of likelihood [0 < likelihood < 1] and consequence)"

1.4.1 "do not include black swan events" (termed the short-term view)

1.4.2 "include black swan events" (termed the long-term view)

1.5 "to contract"

1.5.1 "use build-to-order type"

1.5.2 "use build-to-need type"

1.5.3 "to pay"

1.6 "monitor for short-term and long-term views"

1.6.1 "use short-term operational metrics"

1.6.2 "use short-term operational metrics" [if critical path time for need < net lead times]

1.7 "relate risk to short-term and long-term views"

1.7.1 "define black swan type events for each contract type"

1.7.2 "characterize black swan events into natural and cyber"

1.8 "support process flows"

1.8.1 "communicate to stakeholders"

1.8.2 "coordinate with stakeholders, according to"

1.8.2.1 "stakeholder intent"

1.8.2.2 "stakeholder needs"

Forecasting involves determining the needs of the customer before the supply chain planning occurs. Once customer needs have been determined, then the manufacturer (Blue) can plan to meet the customer's needs by specifying how those demand signals will be satisfied. The overall plan should include means of satisfying normal delivery of goods, including surge request or emergent needs. Reverse logistics is the process of making improvements in the supply chain delivery of goods based on logistic changes, customer demand signal changes, and product returns. Risk is assessed in the supply chain by the determination of likelihood and consequence based on short-term views (non-black swan events), and then by analyses of short-term views and long-term views to ascertain black swan events. The analysis requires monitoring and assessing for short-term and long-term related issues. Contracting is considered separately because it dictates how the demand signal will be met and how much flexibility will Blue have to meet the changes in customer's needs in different scenarios (e.g., Red's attack).

From the short-term and long-term perspectives, these processes are viewed as essential for moving goods among the principle stakeholders, (e.g., the source, suppliers for source, customer, and user). Each process assumes that any cyber-attack is confined individually to the stakeholder that is attacked, without regard for the risk of that stakeholder's involvement with the supply chain (Bowman 2013).

The number of stakeholders in a "simple" supply chain numbers in the hundreds. Referencing the given high level processes, stakeholders and stakeholder types to consider include:

- (ref. 1.1.1) sender of demand signal requires a different, secure channel to confirm order;
- (ref. 1.2.1) who has the problem, what is the genesis of the problem, and why is a problem;
- (ref.1.2.2.3) power company and power distribution company and back-up power vendors;
- (ref. 1.3.2) who has indicated that repurposing of goods is necessary so that reverse logistics can be confirmed with a different, secure channel;
- (ref. 1.4) who are involved with formative, causal actions that may lead to black swan events;
- (ref. 1.5.3) banks involved with transfers of funds or access to accounts to facilitate transfers of funds;
- (ref. 1.6) who are responsible for determining the metrics by which to monitor metrics for strategies related to short-term or long-term perspectives;
- (ref. 1.7) who are responsible for defining and quantifying black swan events, such as solar flares interfering with communications; and
- (ref. 1.8) attorneys involved with communicating with stakeholders regarding computer security policy, and contracts.

As the thinking transitions from short term to long term, the types and number of stakeholders increase due to the addition of seemingly uninvolved stakeholders. For example, an intermediary bank might be seen as a stakeholder who could hold up the transfer of funds to initiate a contract.

Acquisition regulations require that government contracts and work orders be legitimized with transfer of funds. The typically amount of time for a wire transfer is half day for some, three days for most, and up to 15 banking days for settlements of some transfers, including international transactions (assuming all banks are "member" banks of the U.S. Treasury Department) (FCC 2016).

C. SUPPLY CHAINS, A NETWORK MODEL

Based on the technological advances in supply chains and the need to improve efficiency and throughput, conventional supply chain analysis has evolved into modeling supply chain as networks. A simple depiction of a network is illustrated in Figure 4 (Scott et al. 2011).

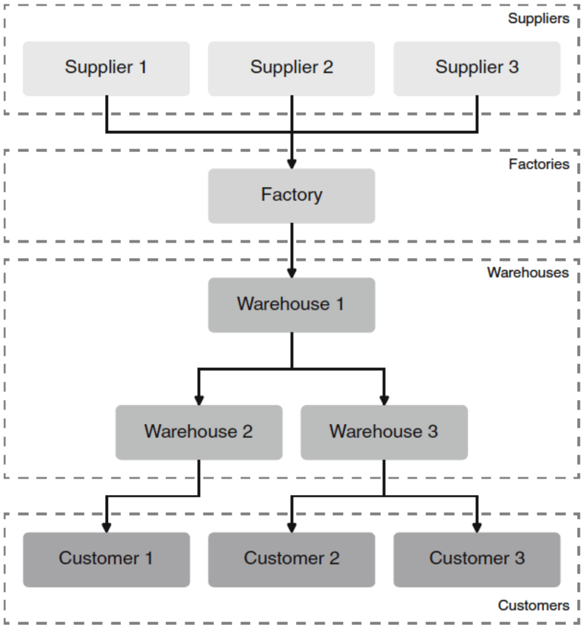


Figure 4. Supply Chain Network Model. Source: Scott et al. (2011).

Due to the increased number of interactions between a greater number of stakeholders, managing the different flows of information, goods, supplies, and components, and transform the interconnectedness of the supply chain into a network of operational models. This complexity is shown in Figure 5. Where, in a simplified depiction, suppliers (squares A, B and C) supply to customer's demands (circles D, E and F) of the network (Goetschalckx 2011). Each channel of flow is indicated by a solid line with an arrow showing the direction of flow, with each channel having different capacity and limitations. The supplier's node generates flow and customer's node consumes flow (Goetschalckx 2011).

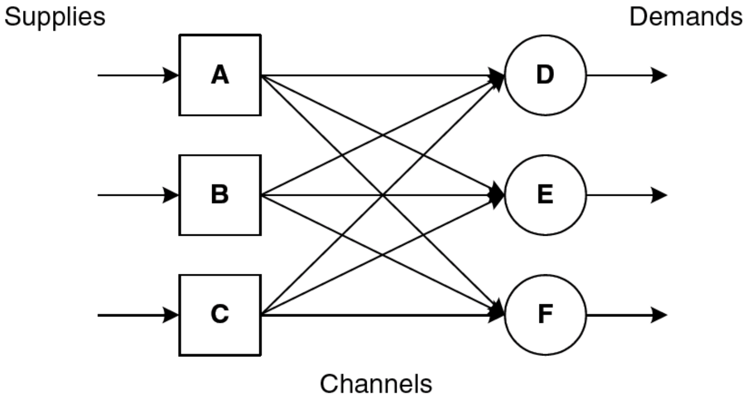


Figure 5. Complexities in the Supply Chain Network, Multiple Origin and Destination. Source: Goetschalckx (2011).

In the supply chain, the process space is then termed a network model, wherein Red may attempt to attack and affect the networks' critical path in both the short-term and long-term views. The critical path determines the time for product delivery, and the total of those paths are defined as the longest path (Goetschalckx 2011). Hence, the critical path should be identified for short-term operations by Blue to apply their limited resources (money and time) in an expeditious manner. From the long-term operational perspective, the critical path view of the short-term is not applicable because any path could be disrupted. With any massive disruption, it is fair to think of all paths as being critical in a massively parallel arrangement and therefore the disruption of one impacts the consequences of all paths (Garcez et al. 2003).

D. SUPPLY CHAIN INPUTS AND OUTPUTS

To determine metrics for a supply chain by which management will determine its status and state of health, the inputs and outputs are outlined in terms of where and when goods flow in the supply chain process model.

The inputs to Supply Chain Model are:

- Product Related Inputs
  - type of goods
  - quantity of goods
  - departure location(s) for goods
  - delivery date(s) for departure of goods at departure location(s)
  - delivery location(s) for goods
  - delivery date(s) for goods arriving at location(s)
  - types of packaging for goods
- Vendor Operations Related Inputs
  - planned Staffing
    - number
    - skills
- Planned Availability of Equipment
  - planned Maintenance
  - planned efficiency of use
- Planned Quality Control of Goods and Delivery
  - quantity of goods that failed inspection
  - type of goods that failed inspection
- Planned Scrap and Rework
  - quantity of goods scrapped

    - type of goods scrapped
    - quantity of goods reworked
    - type of goods reworked
- Planned Time Stored (inventoried)
    - type of goods
    - quantity of goods

The outputs from Supply Chain Model are:

- Product Related Outputs
- Goods Delivered
    - type of goods delivered on time
    - quantity of goods delivered on time
    - type of goods delivered on time with visible damage
    - quantity of goods delivered on time with visible damage
- Goods not Delivered (wrong location (e.g., Shipment errors)
    - type of goods delivered late
    - quantity of goods delivered late
    - delivered late
    - substitute or alternate product delivered
    - wrong part delivered
    - destroyed
    - unaccounted
- Vendor Operations Related Outputs
    - actual staffing hours direct
        - skill mix of labor

    - hourly rate for mix of labor
- actual availability of equipment
    - downtime / wait-time for equipment
    - maintenance time
- actual quality of goods
    - passed / failed inspection
- actual scrap and rework
    - percentage scrap of types of goods
    - percentage rework of types of goods
- actual time stored (inventoried)

E. INITIAL SHORT-TERM BASIC MODEL

It is assumed that Red's intent is to introduce some sort of stressor or stimulus with ultimate goal of gaining insight of the organization's internal process that generate a particular observable event. In this case it can be assumed that Red has unlimited number of resources and is capable of introducing innumerable stimuli and stress on the supply chain. This thesis also assumes that the Red is not aware of the internal processes inside that control the supply chain. Red is in pursuit of a change of state in a causal variable that they can observe. An example of an observable event could be, for example, the Stuxnet worm that would automatically update via the Internet. From the Red's perspective, the observable activity was the successful communication from one of the computers infected and the subsequent update. The attacks can be numerous and may not be predicted. From the perspective of the supply chain attacker, observable events are considered to accurately represent the true state of Blue's operations. Blue is resource constrained in time and money, and it will take an innumerable about of resources to attempt to enumerate every possible observable that the attacker is monitoring. From another perspective, Red may be not be looking for a specific observable, but rather merely looking for what are the observables generated by a specific stress or stimulus placed on the supply chain. Blue must then try to identify the process that seems the most critical. Initially, a critical process is one in which the mission objective is jeopardized when not executed. The model is represented graphically in Figure 6.

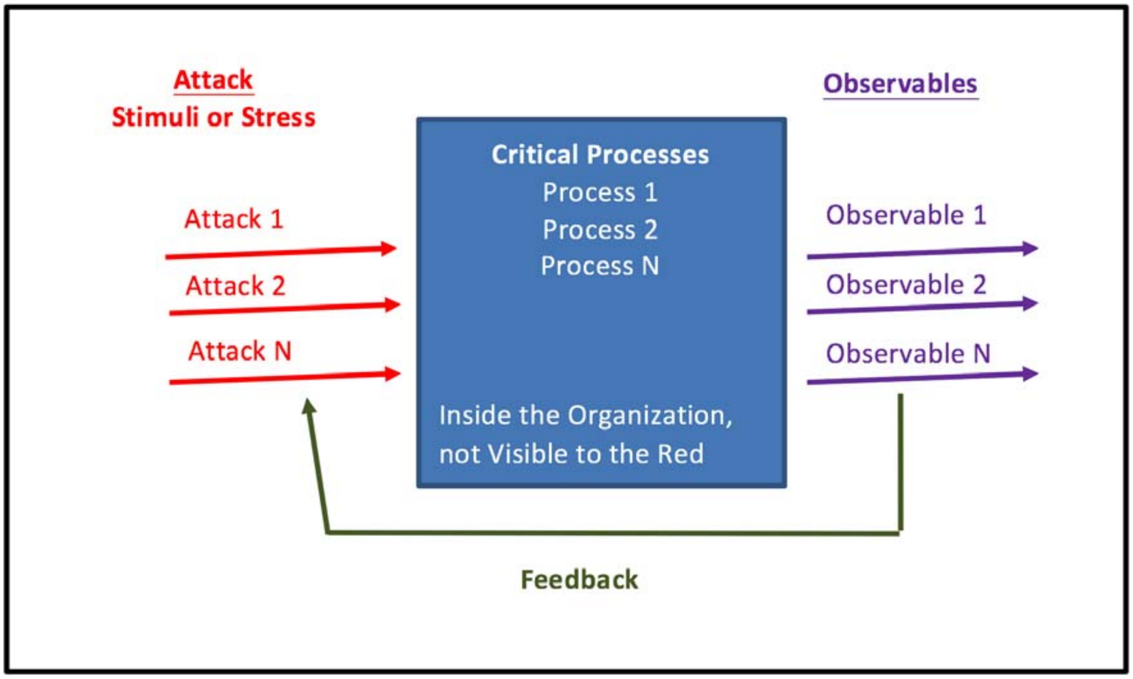


Figure 6. Illustration of the Multitude of Attacks and Observables to Take into Account in the Supply Chain.

1. Short- and Long-term Views Exemplified

Short-term effects are those that provoke an immediate reaction to an event that has recently occurred. From Blue's perspective the model in Figure 6 has no feedback based on the stimulus to the system. Blue believes that once Red initiates an attack on the system, Red has already achieved its goal. Blue then attempts to take corrective action from the stimulus, by developing short-term solutions like software patches, hardware upgrades and or process improvements. Process improvements may have the capability to provide Blue with long-lasting corrective actions. Unfortunately, when most process improvements are developed and implemented, they are developed from the perspective of the initial attack and from what Blue believes was Red’s objective. These improvements most often do not take into consideration the long-terms effects of Red’s attack.

2. Supplier Induced Risks and Supplier Rating: Assessing Risk Based on Selected Metrics

Supplier induced risks, short-term metrics and the supplier’s rating are explained next.

a. Supply Chain Metrics, Short Term

In the general case supply chain management is reactive and stagnant. Reactive from the sense that problems are addressed only when there is a crisis, and the solutions to these problems are short term (Hunter 2012). These short-term approaches lack the depth of analysis required to understand the problem. The Under Secretary of Defense for Acquisition, Technology, and Logistics defines risk management as “an endeavor that begins with requirements formulation and assessment, includes the planning and conducting of a technical risk reduction phase if needed, and strongly influences the structure of the development and test activities ((DASD[SE] 2015).

This section discusses the recommended metrics to be used to assess the supplier’s risk in the short term. These metrics can be used to determine the short-term measures of supplier’s performance. Once the metrics have been identified, then overall risk can be assessed qualitatively. Blue must determine low and risk thresholds based on the availability of resources. These thresholds are set quantitatively. The purpose of the model is to assist Blue in determining the critical processes with high risk.

According to Hunter (2012), for metrics to be effective they should be: received timely (real-time), actionable, focused on vendor’s daily management, comparable to similar data packages from vendors and sub-vendors, simple to gather, and shareable. Based on this criterion the following metrics are suggested to assess the supplier’s effectiveness in the long-term view.

- on-time shipping rate

- on-time delivery of supplier parts from vendor location (Gordon 2008)
- on-time delivery of supplier parts from sub-vendor (Lee, Park, Shin 2009)
- quality of delivery to the vendor from sub vendor (Tuncel, Alpan 2010)
- supply management cost changes (ASD [L&MR] 2016)
- internal quality of materials and parts (SCOR Model)
- overtime for supplier (SCOR Model)
- actual versus planned supplier maintenance hours (SCOR Model)
- on-time delivery of quality corrective actions to vendor from sub-vendor (SCOR Model)
- quality corrective actions to vendor from sub-vendor (SCOR Model)
- inventories (Gordon 2008)
- percentage of expected order that is shipped
- supply backorders (ASD[L&MR] 2016)
- repairs and returns (Teller, Kotzab, Grant 2011)
- shipment errors (Lee, Park, Shin 2009)
- scrap and rework (Gordon 2008)
- planned versus actual staffing (SCOR Model)

A perfectly operating supply chain provides for manufacturing of a sufficiency of goods, storage until needed, transfer and delivery of goods according to valid orders to correct locations on time. Using the metrics provided, a perfect supply chain would allow the supplier to have: a high shipping rate, on time deliveries, high quality products, low overtime, equal and planned maintenance hours. An imperfectly operating supply chain would not correctly deliver orders on time. An imperfect supply chain is more expensive than the defined perfect supply chain.

The following metrics can be used by Blue to determine the physical and cybersecurity responsiveness to attack. From the perspective of short-term thinking, these metrics are lagging indicators of attacks and as such serve to determine how well prepared Blue is to deal with changing Red attacks.

- time to identify attack
- time attack continued unnoticed
- time to respond to attack
- time to respond to susceptibility
- time to respond to vulnerability
- time to assess and evaluate vulnerability
- time to assess and evaluate susceptibility
- time to implement security fix (cyber or physical)
- number of related incidents over time (short-term focus on the specifics of the immediate attack)
- types of related incidents over time (long-term focus on the implications of short-term attacks)

From the perspective of long-term thinking, these metrics can suggest the speed in which Blue must react surreptitiously to prohibit or lessen a complete collapse of the supply chain.

If in the short term, the time to identify attacks, rectify susceptibilities, and decrease vulnerabilities, the long-term risk may increase. The increase occurs because the consequences of Red's attacks may not be assessed. The early inability to detect Red's attacks changes the trajectory of Blue's response. It is of little solace that new tools are being implemented to detected if an attack has occurred (Committee on Oversight and Government Reform 2015). However, in the short term, the attacks are identified immediately and no data or information is lost, then the long-term risks may decrease. The decrease occurs because Red's attacks are thwarted, and Blue's system remains unscathed. The counter argument to these increases and decreases is that Blue allows Red to access a controlled portion of supply chain network, fully knowing that in this controlled environment, Red's attack can be monitored and evaluated.

b. Anatomy of a Cyber-Attack

Any registered domain (text version of an Internet protocol (IP) or numeric address) on the collection of networks (referred to as the Internet), links computers that can access software programs that manage, retrieve, and store information and data. Any domain is a target for cyber-attacks. According to Joe Zott, who help establish the anti-tamper program at the National Security Agency, there are three steps to a cyber-attack—learn the target, identify vulnerabilities and susceptibilities, and plan the attack (Zott 2008).

1. Learning the target means to check for common computer hosts of information, data, and executable software; identify the number of hosts and IP addresses, (e.g., Host 208.144.58.14); and the type of protocol (active or passive file transfer protocol, FTP and protocol to establish a remote terminal (telnet)); along with status of each communication ports (open/closed).

2. Identifying vulnerabilities for each server means identifying the state of operations and the services and remote procedures running on the various types of communications ports (e.g., Port: 21) TCP—State: open msrpc (Microsoft remote procedure call, and Port: 8089/TCP—blackICE-ICEcap, where TCP is the standard Internet transmission control protocol and blackICE-ICEcap is anti-hacker software designed to protect against intrusion into enterprise networks). Each service has known and exploitable vulnerabilities. The degree of susceptibility is then determined by the amount of access gained through successful passwords (for example), the level of control that is taken, and the kind of masking that will be effective in hiding the intrusion.

3. Planning the attack takes advantage of the enterprise architecture, vulnerabilities, and susceptibilities. Gaining access to and control of the supply chain enterprise management may be through a supplier, banker, insurance carrier, or any number of stakeholders commonly deemed external to the enterprise network. Each of these "external" stakeholders are integral to the operations, but not necessarily on a day-to-day basis. Yet, external stakeholders should be considered as part of the internal operations of the supply chain computer management system.

An often-employed strategy for Red is to interrogate the supply chain with attacks immediately after a security update to find and exploit susceptibilities before the next security update. Updates make changes that need to be evaluated in order to continue making cyber-attacks. The earlier Red adapts to changes in Blue's system, the more time Red has to adapt and further attack the supply chain. Consequently, Blue needs to be most vigilant after security updates. The National Cyber Alert System hosted by the Department of Homeland Security offers products for current activity, alerts, bulletins, and tips (https://www.us-cert.gov/ncas).

Planning the attack can be posed as a short-term tactic within a long-term strategy. There are typically five reasons for an attack in the short term—ranging from profiting from the sale of information to complete destruction of Blue's enterprise capability (Zott 2008). The five broad categories of attacks are:

- to gain control of a computer(s) to be used for future attacks or to sell information to other hackers
- to obtain information
- to modify information
- to obtain service (e.g., to send a fraudulent email)
- to implement denial of service by flooding bandwidth with messages, producing malformed packets, or by corrupting or changing the translation of domain name into the IP address.

Information gained in the short-term can be used in the long-term.

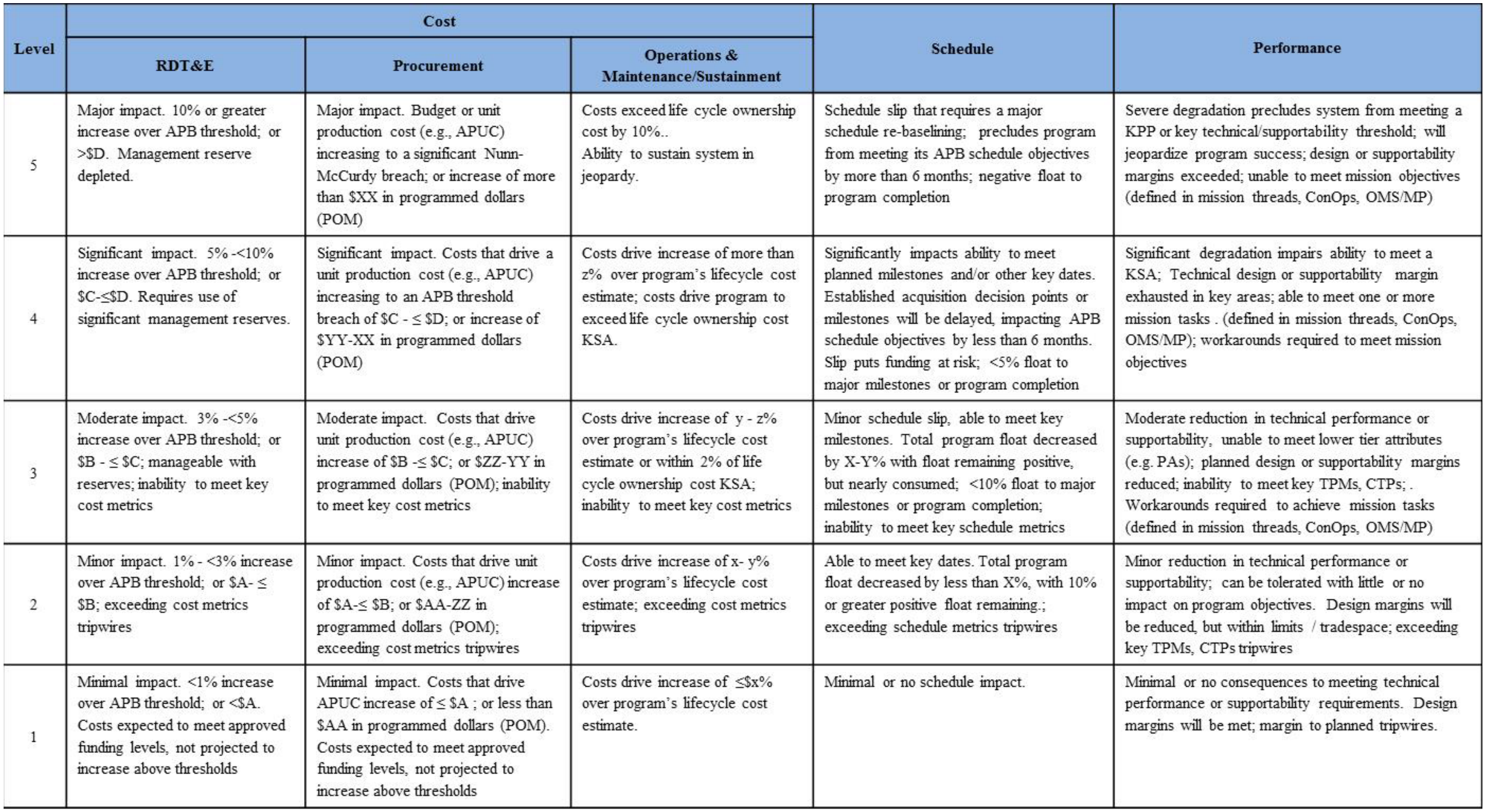
According to the DOD Risk Management Guide (DASD[SE] 2015), Blue can assess each of the suppliers involved with the supply chain by assigning a risk within a 5x5 matrix made up of five levels of likelihood and five levels of consequence. The supplier's performance is directly related to assessing the results of documented performances as collected and characterized as metrics. Table 1 illustrates the recommended likelihood criteria and Table 2 indicates the levels of consequence. Both tables are adapted to cyber risk where it is preferred that the probability of occurrence is based on systems engineering analyses rather than the opinion of subject matter experts.

Table 1. DOD Recommended Likelihood Criteria. Source: DASD(SE) (2015).

Level	**Likelihood**	**Probability of Occurrence**
5	Near Certainty	> 80% to ≤ 99%
4	Highly Likely	> 60% to ≤ 80%
3	Likely	> 40% to ≤ 60%
2	Low Likelihood	> 20% to ≤ 40%
1	Not Likely	> 1% to ≤ 20%

The DOD Risk Management Guide stipulates that "programs also consider the effect of aggregated risk on a program." This thesis interprets that DOD guidance as considering the long-term perspective as well as the short-term perspective.

Table 2. DOD Recommended Structure for Categorizing Consequences. Source: DASD(SE) (2015).



Level	Cost			Schedule	Performance
	RDT&E	Procurement	Operations & Maintenance/Sustainment		
5	Major impact. 10% or greater increase over APB threshold; or >$D. Management reserve depleted.	Major impact. Budget or unit production cost (e.g., APUC) increasing to a significant Nunn-McCurdy breach; or increase of more than $XX in programmed dollars (POM)	Costs exceed life cycle ownership cost by 10%.. Ability to sustain system in jeopardy.	Schedule slip that requires a major schedule re-baselining; precludes program from meeting its APB schedule objectives by more than 6 months; negative float to program completion	Severe degradation precludes system from meeting a KPP or key technical/supportability threshold; will jeopardize program success; design or supportability margins exceeded; unable to meet mission objectives (defined in mission threads, ConOps, OMS/MP)
4	Significant impact. 5% -<10% increase over APB threshold; or $C-≤$D. Requires use of significant management reserves.	Significant impact. Costs that drive a unit production cost (e.g., APUC) increasing to an APB threshold breach of $C - ≤ $D; or increase of $YY-XX in programmed dollars (POM)	Costs drive increase of more than z% over program's lifecycle cost estimate; costs drive program to exceed life cycle ownership cost KSA.	Significantly impacts ability to meet planned milestones and/or other key dates. Established acquisition decision points or milestones will be delayed, impacting APB schedule objectives by less than 6 months. Slip puts funding at risk; <5% float to major milestones or program completion	Significant degradation impairs ability to meet a KSA; Technical design or supportability margin exhausted in key areas; able to meet one or more mission tasks . (defined in mission threads, ConOps, OMS/MP); workarounds required to meet mission objectives
3	Moderate impact. 3% -<5% increase over APB threshold; or $B - ≤ $C; manageable with reserves; inability to meet key cost metrics	Moderate impact. Costs that drive unit production cost (e.g., APUC) increase of $B -≤ $C; or $ZZ-YY in programmed dollars (POM); inability to meet key cost metrics	Costs drive increase of y - z% over program's lifecycle cost estimate or within 2% of life cycle ownership cost KSA; inability to meet key cost metrics	Minor schedule slip, able to meet key milestones. Total program float decreased by X-Y% with float remaining positive, but nearly consumed; <10% float to major milestones or program completion; inability to meet key schedule metrics	Moderate reduction in technical performance or supportability, unable to meet lower tier attributes (e.g. PAs); planned design or supportability margins reduced; inability to meet key TPMs, CTPs; . Workarounds required to achieve mission tasks (defined in mission threads, ConOps, OMS/MP)
2	Minor impact. 1% - <3% increase over APB threshold; or $A- ≤ $B; exceeding cost metrics tripwires	Minor impact. Costs that drive unit production cost (e.g., APUC) increase of $A-≤ $B; or $AA-ZZ in programmed dollars (POM); exceeding cost metrics tripwires	Costs drive increase of x- y% over program's lifecycle cost estimate; exceeding cost metrics tripwires	Able to meet key dates. Total program float decreased by less than X%, with 10% or greater positive float remaining.; exceeding schedule metrics tripwires	Minor reduction in technical performance or supportability; can be tolerated with little or no impact on program objectives. Design margins will be reduced, but within limits / tradespace; exceeding key TPMs, CTPs tripwires
1	Minimal impact. <1% increase over APB threshold; or <$A. Costs expected to meet approved funding levels, not projected to increase above thresholds	Minimal impact. Costs that drive APUC increase of ≤ $A ; or less than $AA in programmed dollars (POM). Costs expected to meet approved funding levels, not projected to increase above thresholds	Costs drive increase of ≤$x% over program's lifecycle cost estimate.	Minimal or no schedule impact.	Minimal or no consequences to meeting technical performance or supportability requirements. Design margins will be met; margin to planned tripwires.

Low risk is assigned to a supplier's score less than a predetermined low-risk threshold. Medium risk is assigned to a supplier's score within the low- and high-risk thresholds. Finally, high risk is assigned to a supplier whose score is higher than the predetermined high-risk threshold.

The consequences of the short-term attack can be structured in the format shown in the DOD Risk Management Guide. Table 3 illustrates the adaptation of the DOD categorization of consequences.

Table 3. Adaptation of the DOD Categorization of Consequences. Adapted from DASD(SE) (2015).

Short-term Consequences			
Level	Function	Performance Consequence	Schedule
1	Produce goods	- wrong parts ordered from vendor - no parts ordered from vendor - parts ordered from wrong vendor	Short-term duration
	Manufacture goods	- no electricity - labor shortage (illness, labor strife, civil unrest)	
	Store goods	- parts/goods put into wrong location - retrieved wrong parts from right location	
	Ship goods	- goods loaded into wrong transport vehicle - vehicles do not arrive (no request received, sent to wrong location, sent at a different time than requested)	
	Receive goods	- wrong parts (misidentified, or wrong) - insufficient number	

When only a few goods or parts fall into the performance consequences indicated in Table 3, with a brief interruption in schedule of delivery for the supply chain, the user's activities may be minimally affected. A level 1 risk is indicated for these cyber-attacks since the criticality of delivery typically involves routine work-arounds. As the number of consequences increases, the user may experience greater impacts from the malfunctioning supply chain. The short-term view may be several “small” impacts that are not considered remarkable in and of themselves. As the number of problems in the supply chain increase and the consequences increase, the categories of severity increases and the risks increase.

From the cybersecurity and supply chain perspective, cost will be dependent on the level of research needed to develop, produce and/or operate, maintain and sustain new software and/or hardware. Schedule impacts depend on the effects of cybersecurity on the schedule of delivery of acquisition milestones, decision points and program completion. The level of performance is degraded when the cybersecurity affects the technical performance of hardware or software at is relates to customer requirements. The concepts of cost, schedule, and performance can be tailored to the cybersecurity situation where the supply chain is moving goods during several types of situations. For example, “normal supply” for supporting mission’s operations; and “critical supply” during emergencies will provide Red with operational situations and response to typical problems. A normal supply situation is one which the supplier supports the user’s need as required by the customer (Blue). The critical supply scenario occurs either when the user requires immediate delivery of a product due to emergency repairs or because the supply chain was not able to deliver as required.

Now assume that a short-term attack is meant for Red to accomplish one or more of the following (in order):

1. Discover the servers that participate in Blue supply chain
2. Learn the names of the servers and their associated passwords to gain access
3. Map the architecture of the servers
4. Identify the participants
5. Identify the routing of messages to transfer goods

From the supply chain perspective, assume that Blue wants to assess the risk on Red's ability to discover the servers in Blue's supply chain (Risk #1) and learn server names and passwords (Risk #2). Based on this information, Blue assumes that based on historical data and current security protocols, and determines that Risk #1 and #2 have a probability of occurrence of 65% and 35%, respectively. Based on these probabilities and using Table 2, then, Risk #1 and #2, have a risk likelihood level 4 and 2, respectively. These results are highlighted on Table 4.

Table 4. Likelihood Criteria for Risk #1 and #2.
Adapted from DASD(SE) (2015).

Level	Likelihood	Probability of Occurrence	Risk
5	Near Certainty	> 80% to ≤ 99%	
4	Highly Likely	> 60% to ≤ 80%	#1
3	Likely	> 40% to ≤ 60%	
2	Low Likelihood	> 20% to ≤ 40%	#2
1	Not Likely	> 1% to ≤ 20%	

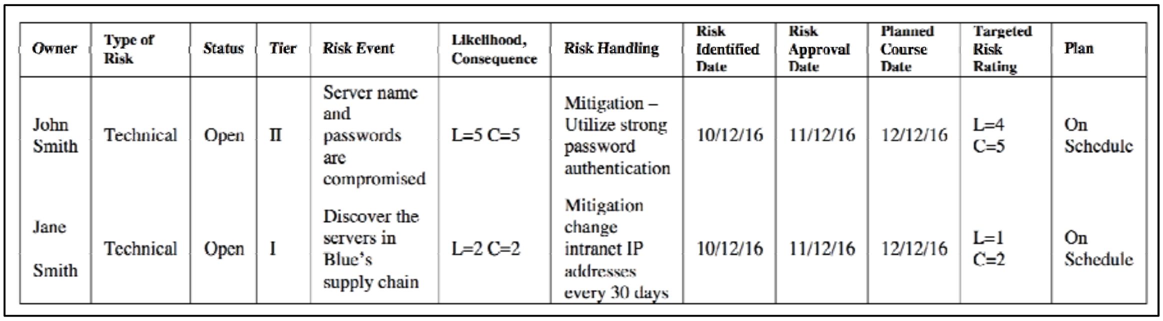
Blue assesses the consequences for Risk #1 and #2 based on the impact on cost, schedule and performance. Risk #1 and #2 have major and minor impact, respectively. If the server name and passwords are compromised (Risk #1), the resulting impact will critically affect the cost of repair, delivery schedules and the subsequent ability to make future deliveries. If the server locations are compromised (Risk #2), Blue assumes that the overall impact is minor since knowing the server location may have a minor impact on cost (server's Internet protocol (IP) address can be changed), schedule (changing the IP address may take a couple of hours) and performance (little to no effect on the delivery of goods and services). A summary of those results are illustrated on Table 5. In summary Risk #1 has a likelihood of level 2 and consequence of level 5. The same methodology can be applied to Risk #2, which has a likelihood of level 2 and consequence of level 2.

Table 5. Consequence Criteria for Risk #1 and #2. Adapted from DASD(SE) (2015).

Level	Cost	Schedule	Performance	Risk
5	Major Impact	Major Impact	Major Impact	#1
4	Significant Impact	Significant Impact	Significant Impact	
3	Moderate Impact	Moderate Impact	Moderate Impact	
2	Minor Impact	Minor Impact	Minor Impact	#2
1	Minimal Impact	Minimal Impact	Minimal Impact	

Once Blue has determined mitigating measures for all identified risks, then the likelihood and consequence can be recorded in Risk Register for traceability of risks and their associated rating (DASD[SE] 2015), as shown in Table 6. Blue assessed that based on their risk strategy, the likelihood of Risk # 1 and #2 occurring is reduced to level 3 and 1, respectively. Likelihood is indicated as an L, and consequence as a C in Table 6.

Table 6. Supplier Risk Levels Based on Quantitative Metric Performance. Adapted from DASD(SE) (2015).



Owner	Type of Risk	Status	Tier	Risk Event	Likelihood, Consequence	Risk Handling	Risk Identified Date	Risk Approval Date	Planned Course Date	Targeted Risk Rating	Plan
John Smith	Technical	Open	II	Server name and passwords are compromised	L=5 C=5	Mitigation – Utilize strong password authentication	10/12/16	11/12/16	12/12/16	L=4 C=5	On Schedule
Jane Smith	Technical	Open	I	Discover the servers in Blue's supply chain	L=2 C=2	Mitigation change intranet IP addresses every 30 days	10/12/16	11/12/16	12/12/16	L=1 C=2	On Schedule

Once improvements are put in place, based on assessed corrective actions, Blue can use the same metrics to determine the effectiveness of these improvements. The model may also be used to compare critical processes and determine which process improvement is most effective under limited resources.

THIS PAGE INTENTIONALLY LEFT BLANK

III. LONG-TERM SUPPLY CHAIN VULNERABILITY

The topic of long-term success for a supply chain is predicated on having measured, quick responses to cyber-attacks that are effective in sustaining a near-perfectly operating supply chain. User and mission are neither impacted by the responses to the cyber-attacks nor by the solutions that are implemented. Knowing what to do and how to overcome the problems derive from the experiences offered by the portending events exposed during the short-term cyber-attacks. The approach of preparing for a black swan event is rooted in these short-term cyber-attacks.

There would seem to be no expeditious way to prepare for a completely dysfunctional supply chain other than to have all of the required parts for any use at the right location all the time. The practical nature of providing all parts at the right location all the time is near-impossible to determine for all future events and likely prohibitively expensive. Preparing for a black swan event is rightly considered as an integral part of the long-term perspective. Rather than predicting the consequences of uncertainty, the DOD risk framework combines with the functional nature of the supply chain to afford a view of the vulnerabilities to cyber-attack. The short-term breakdowns in the supply chain provide the basis for fixing system problems in the supply chain architecture. The functional description of “to manufacture,” “to store,” “to move,” “to accept” provides a description of how cyber-attacks can disrupt each function, labelled “consequence” (Table 3 from Chapter II). The short-term risk differs from the long-term risk, thereby the mix and match of the short-term cyber-attacks can be modeled into combinations that degrade the supply chain functions for a long-term black swan event. To prepare for the black swan, what needs to be fixed in the supply chain needs to be broken in the short term or anticipated to be broken in the short term. Through the functional perspective used in systems engineering, there is no need to predict uncertainty. When a portion of the supply chain is broken, it needs to be fixed in concert with the survival of the whole supply chain, not just the portion that was broken.

A. LONG-TERM VIEWS—A BLACK SWAN EVENT: THE IMPACTS OF IMPROBABLE EVENTS

Uncertainty in information and data concerning the vulnerability of a supply chain to cyber-attacks results in decision risk, operational risk, programmatic risk, and technical risk (Ullman 2009). Uncertainty in managing the outcomes of directing and controlling a supply chain depend on measuring the functional performance against the short-term and long-term metrics, while taking into account any uncertainty in forecasts or assessing risks. The concept of risk can be thought of as a continuous function, with probability distribution functions providing a convenient mapping between intervals of possible events and probabilities or likelihood of occurrence. The basis of risk is the uncertainty in the variables that are causal to the events that we fear for loss or injury—for this research, the functional architecture that makes the supply chain vulnerable to cyber-attacks.

Anna Orlik and Laura Veldkamp, writing for the U.S. National Bureau of Economic Research (Orlik and Veldkamp 2014) showed that significant fluctuations in uncertainty can be seen in the Gross Domestic Product data from 1947 to 1968—indicative of black swan events. Black swan events are detectable in the skewness of a distribution (Orlik and Veldkamp 2014). The probability distribution functions used by professional forecasters are traditionally symmetrical (Gaussian). Gaussian mathematics is straightforward and supported by readily available statistical software, making the calculations within the reach of forecasters. However, the probability distribution functions derived from the quarterly economic data were asymmetrical (i.e., non-Gaussian). Orlik and Veldkamp showed that by separating the parameter updating from the skewness the uncertainty rose with each stressor in the economy (i.e., caused by each economic recession). That uncertainty was strongly correlated with the defined event, the black swan. Upsurges in uncertainty were shown to correspond with probability of “long tail” events, as expressed by increases in skewness (Taleb 2010; Orlik and Veldkamp 2015) over that of non-stressor imbued data.

Causes of increased uncertainties arise in managing a supply chain include overrunning budgets (causes misunderstood), missing delivery milestones (causes ascribed incorrectly), insufficiency of skilled personnel (inadequate management communications), ineffective process controls, and vulnerability to cyber-attacks, for example. In general, any action that impacts the linear nature of scheduling activities, commensurate with budgetary and functional performances, leads to non-linear effects that increase the likelihood of uncertainty. Yet, none of these listed items are black swans.

B. LONG-TERM PROCEDURES AND MODEL

Referencing the short-term model, Red's intent is to introduce a stressor or stimulus to gain insight of the Blue's internal process and computer operations that generate particular observables. Observables that are visible within the organization and can be discerned through the exchange of communications on the computer network(s), and those observables that can be detected externally are feedbacks that Red requires to learn about the effectiveness of cyber-attacks. That is to say, if Red did not receive feedback as to the effectiveness of their cyber-attacks, then the impacts on the supply chain many not be discernable, and Red may change their attack schemas.

In summary, Blue assumes that Red has unlimited number of resources is capable of introducing innumerable stimuli and stresses to interrogate the supply chain. The stress or stimulus triggers an internal process that produces an observable event, and Blue's internal process inside the supply chain may or may not be seen by Red. For example, the long-term objective for Red in Stuxnet was to take control of the digital computers used for plant's automation. Red's focus was to increase the speed to the centrifuges to cause mission failure, due to several short-term stresses on the system (e.g., infecting one of the plant's computers operating system to multiply the Stuxnet worm and reach across multiple computers in the long-term). The long-term objective for Blue is to then try to identify the processes that seem to be most critical. Criticality can usually be found in a few processes or in an aggregation of well-time failures that freeze operations of the supply chain. The long-term model is represented graphically in Figure 7.

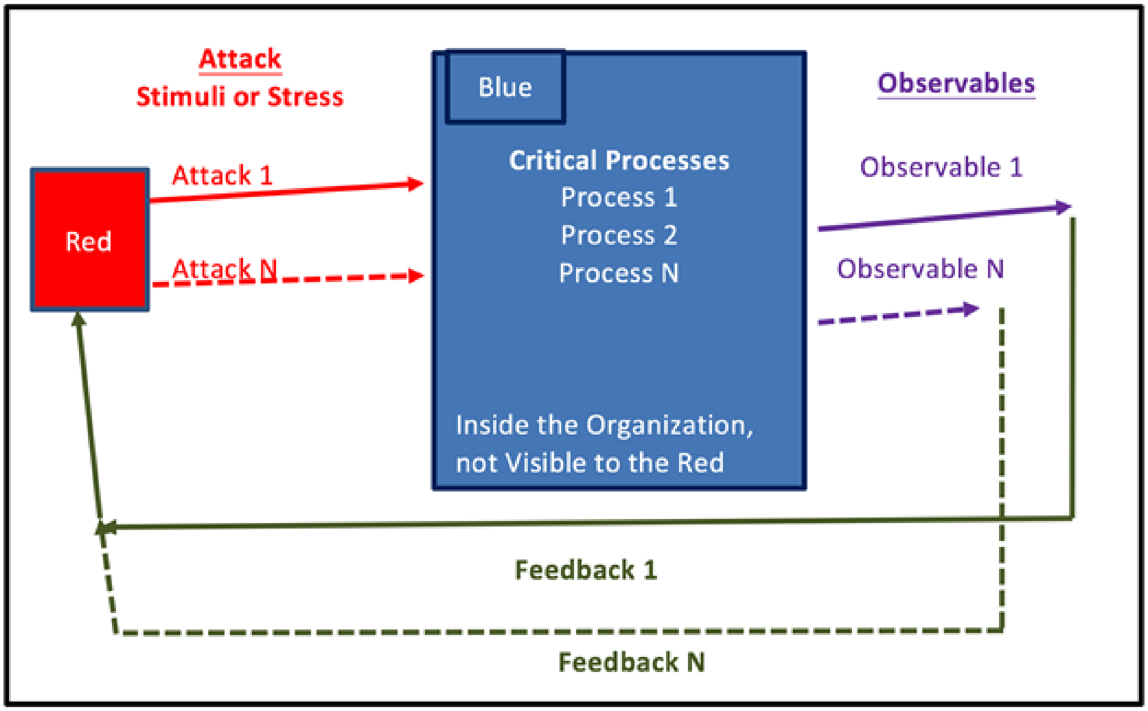


Figure 7. Long-term Model Illustration of the Multitude of Attacks and Observables on the Supply Chain.

For long-term objectives. Red will generate one attack (Attack 1) on the system that eventually causes Blue to respond and cause an external observable (Observable 1). Observable 1 is monitored and fed back (Feedback 1) to Red. Red in turn generates subsequent attacks (in series, parallel, single or simultaneous) denoted as Attack N, which generates an Observable N, and fed back N number of times. The process continues where Blue may not notice the interrelation between the attacks. At a future time, Red decides to initiate all or a series of attacks to attain an effect (black swan) to causing mission degradation. Notice the difference in the feedback loop in the long-term versus short-term objectives. For long-term objectives, the feedback provides the initial conditions for the next attack. The short-term objectives, offer feedback to provide observable events for Red, it ends there. From Blue's perspective the multiple attacks may not be related.

The final impact on Blue in the long term is that the supply chain process ceases to function as a perfect supply chain. In order to restart the flow of goods and parts through the supply chain, it may require new sources of equipment and new acquisitions, since the existing suppliers may not be able to deliver when designated.

C. SOURCES OF UNCERTAINTY

Orlik and Veldkamp define a black swan event as one that exhibits uncertainty fluctuations, caused by "time-varying risk of unobserved tail events" (Orlik and Veldkamp 2015, 2), in other words a "conditional probability of a rare event" (2015, 4). These "tailed" events related to the thickness of the expected distribution tails, also known as skewness. Such fluctuations assume that the true distribution of supply chain vulnerabilities occur as unknowns. The significant contribution of Orlik and Veldkamp was to explain large fluctuations in uncertainty as due to changes in the likelihood of events that were distributed far from the mean of the data. Through a careful analysis of the causes of statistical significance, Orlik and Veldkamp discovered, it was not changes in the variance in the data that was the culprit, but an associated risk with black swans. "Thus, everyday fluctuations in a data series can produce large fluctuations in conditional variance for an agent who is constantly re-estimating the tails of the distribution," (Orlik and Veldkamp 2015, 1).

For black swan events, as defined by Orlik and Veldkamp, uncertainty (U_{it}) is the variance of the expected value of the expected metric recorded data point (y_{t+1}) at time t+1 minus the forecasted metric expected value $E(y_{t+1}|I_{it})$ given new information (I_{it}) (2015). The equation for U_{it} is shown in Figure 13.

$$U_{it} = \sqrt{E\left[\left(y_{t+1} - E[y_{t+1}|\mathcal{I}_{it}]\right)^2 \middle| \mathcal{I}_{it}\right]}.$$

Figure 8. Uncertainty. Source: Orlik, Veldkamp (2015).

The forecasted metric value $y_{t+1}|I_{it}$ is defined as the probability of the next data point (y_{t+1}) given the new information received changed the perception (I_{it}), where the growth y_{t+1} is for all information captured through each period of time *t*.

Volatility (V_t) is defined as variance of uncertainty, taking into consideration that unexpected data value collected (y_t). The forecasting Model (M) has a vector of parameters (θ). Every M has agent i's information in set I_{it} that incorporates the volatility based on history y^t, the Model M, and the parameters θ. The equation for V_t is shown in Figure 14.

$$V_t = \sqrt{E\left[(y_{t+1} - E[y_{t+1} | y^t, \theta, \mathcal{M}])^2 \middle| y^t, \mathcal{M}, \theta \right]}.$$

Figure 9. Volatility. Source: Orlik, Veldkamp (2015).

The square of uncertainty is equal to the expected squared forecast error (Orlik, Veldkamp 2015, 9). There are six traditional strategies for the Model M forecasting model to manage the movement of goods through the supply chain, termed (Perez 2013):

- efficient supply chain model—driven by customer demand with outbound logistics to maintain inventory in transit to satisfy surge needs.
- fast supply chain model—geared for short life-cycle products with production of goods scheduled in batches.
- continuous-flow supply chain model—relies on stability in supply and demand to provide for a steady flow of goods, with little variation in the same set of goods.
- agile supply chain model—driven by customer for goods with unique specifications, often stimulated by unpredictable demand, and resulting in excess goods in the supply chain.
- custom-configured supply chain model—driven by the a high ratio of cost of assets to the total cost of the totality of the supply chain because of the high-degree of configurability of goods to satisfy a mix-and-match requirement that varies from user to user.
- flexible supply chain model—structured to deliver goods with demands that cannot be forecasted, resulting in delays for deliveries, periods of high volume work and low volume work, and noted for responding to unexpected situations.

While customers may want to have all six strategies at least possible within their supply chain architecture, the agglomerated result will offer no one strategy in an optimized fashion, with some strategies found to be distinctly underperforming (Perez 2013).

Without choosing a specific model for this thesis, the model for the efficient supply chain is examined to investigate long-term issues resulting from cyber-attacks.

D. LONG-TERM METRICS

The equation for volatility (V_t) is used to set thresholds for each event that stress the supply chain. The following metrics can be used by Blue to determine the physical and cybersecurity responsiveness to an attack. These metrics are forecasting/leading indicators of attacks. Attacks on the supply chain that lead to overall catastrophic supply chain failures (e.g., communication malfunctions, delivery of wrong goods to various locations, and consequences indicated in the short-term consequence table) can be measured as follows:

- percent of correct goods that leave on time
- percent of correct delivery of goods at proper location
- percent of goods damaged in transit
- percent of goods that are missing from inventory
- estimated time to restore communications problems
- estimated time to locate missing goods
- estimated number of wrong parts that might be delivered
- probability of misled decisions
- estimated degree of effectiveness in carrying out proper analysis and evaluation of supply chain problems (i.e., status of activities if multiple functional failures occur)

As with the short-term consequences, the long-term attack can be structured similarly in the format shown in the DOD Risk Management Guide. Table 7 illustrates the adaptation of the DOD categorization of long-term consequences. For long-term effects, there is combination of events from multiple functions. For example, multiple unrelated parts from multiple vendors do not arrive when critically needed, and multiple unrelated labor shortage (illness, labor strife, civil unrest) occur at multiple locations at the same time causing mission failure. The term “unrelated” implies that Blue is not aware of the implications of the event nor does not find the correlation in the events. The likelihood for long-term problems is shown in Table 8.

Table 7. Adaptation of the DOD Categorization of Consequences for Long-term. Adapted from DASD(SE) (2015).

Long-term Consequences			
Level	Function	Performance Consequence	Schedule
Scale the consequences from 5 (high) to 1 (low) as the situation is assessed as changing from the short-term perspective	Produce goods	Multiple unrelated parts: - from multiple vendors don’t arrive when critically needed. - from multiple vendor are not ordered - ordered from wrong multiple vendors	Long-term duration (e.g., Mission failure)
	Manufacture goods	Multiple unrelated : - electrical faults generate power failure at multiple locations in the supply chain - labor shortage (illness, labor strife, civil unrest) occur at multiple locations	
	Store goods	Multiple unrelated: -parts/goods put into wrong locations - retrieved wrong parts from right locations	
	Ship goods	- Multiple unrelated goods loaded into wrong transport vehicles from different vendors	
	Receive goods	Multiple unrelated: -vehicles do not arrive (no request received, sent to wrong location, sent at a different time than requested) - wrong parts (misidentified, or wrong) received - insufficient number received	

From the supply chain perspective, Blue determines that a problem is detected in the type of goods that are planned to be transited to a location with an urgent need. This behavior has been observed before and Red is suspected to be perpetrating a cyber-attack (Risk #1). Subsequently, communications is lost with another user (also an infrequent event) (Risk #2). The temporal proximity of the two risks is cause for suspicion and an analysis of the long-term consequences is initiated. Based on this information, Blue assumes that the historical data and current security protocols are undermined by a cyber-attack and further that Risk #1 and #2 have a probability of occurrence of 75% and 80%, respectively. Based on these probabilities and using Table 1, then, Risk #1 and #2, both have a risk likelihood of level 4. Appropriate, planned actions are then taken by Blue to continue transiting appropriate goods to proper locations. These results are highlighted in Table 9.

Table 8. Likelihood Criteria for Risk #1 and #2.
Adapted from DASD(SE). (2015).

Level	Likelihood	Probability of Occurrence	Risk
5	Near Certainty	> 80% to ≤ 99%	
4	Highly Likely	> 60% to ≤ 80%	#1, #2
3	Likely	> 40% to ≤ 60%	
2	Low Likelihood	> 20% to ≤ 40%	
1	Not Likely	> 1% to ≤ 20%	

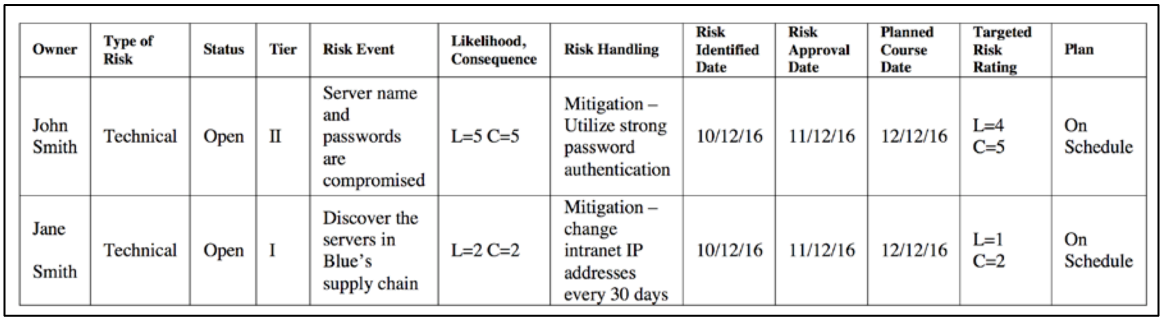
Blue assesses the consequences for Risk #1 and #2 based on the impact on cost, schedule and performance. Risk #1 and #2 have a combined significant impact. A summary of those results are illustrated in Table 10. In summary Risk #1 has a likelihood and consequence level of 4 and 5 respectively, then L=4 and C=4. The same methodology an be applied to Risk #2, which has a likelihood and consequence of L=4 and C=4.

Table 9. Consequence Criteria for Risk #1 and #2. Adapted from DASD(SE). (2015).

Level	Cost	Schedule	Performance	Risk
5	Major Impact	Major Impact	Major Impact	
4	Significant Impact	Significant Impact	Significant Impact	#1, #2
3	Moderate Impact	Moderate Impact	Moderate Impact	
2	Minor Impact	Minor Impact	Minor Impact	
1	Minimal Impact	Minimal Impact	Minimal Impact	

Once Blue has determined mitigating measures for all identified risks, then the likelihood and consequence can be recorded in Risk Register (Table 10) for traceability of risks and their associated rating (DASD[SE] 2015). Blue assessed that based on their risk strategy, the likelihood of Risk # 1 and #2 occurring is reduced to level 3 and 1, respectively.

Table 10. Risk Register for Traceability of Risks and Their Associated Rating. Adapted from DASD(SE) (2015).



Owner	Type of Risk	Status	Tier	Risk Event	Likelihood, Consequence	Risk Handling	Risk Identified Date	Risk Approval Date	Planned Course Date	Targeted Risk Rating	Plan
John Smith	Technical	Open	II	Server name and passwords are compromised	L=5 C=5	Mitigation – Utilize strong password authentication	10/12/16	11/12/16	12/12/16	L=4 C=5	On Schedule
Jane Smith	Technical	Open	I	Discover the servers in Blue's supply chain	L=2 C=2	Mitigation – change intranet IP addresses every 30 days	10/12/16	11/12/16	12/12/16	L=1 C=2	On Schedule

IV. CONCLUSION AND RECOMMENDATIONS

A life-cycle approach to successful supply chain vulnerability assessment includes in-depth analysis of both short-term and long-term metrics. Short-term views may be used as mitigation factors and to conduct immediate corrective actions to address a found vulnerability. Unfortunately, these short-term actions may fall short in attempting to determine or even assess what are or could be Red's long-term objectives. Red's long-term objectives may not be driven by the immediate rewards of the short-term attack, but rather to collect information to be used in the future. At the time of the short-term attack, Red may not explicitly know what is its long-term objective, but may be formulating it as they progress though short-term cyber-attacks. But when the time comes in the future, where Blue's mission degradation is needed, Red may trigger a series of attacks.

Short-term responsiveness to cyber-attacks on supply chains can be boosted by identifying the thresholds on long-term effects, black swan events can be postulated from the metrics for short-term cyber-attacks. Since long-term dangers of black swan events are meant to destroy supply chain effectiveness for a critical period, the types of black swan events identified in this thesis are meant to be combinations of the short-term problems typically faced during cyber-attacks.

The black swan events can be identified by mapping the short-term metrics (e.g., percentage of expected order that is shipped, repairs and returns or scrap and rework) into long-term metrics (combinations of expected order that is shipped, repairs and returns, and scrap and rework). In other words, various short-term metrics need to be monitored by Blue to be interpreted as an attack to intentionally deceive and achieve a long-term objective. Deceive by Red with short-term cyber-attacks; Blue believed there was no problem in shipping items. Blue was confident that all fixes from the short-term cyber-attacks were effective. However, Red had inserted sophisticated software code, that when activated in the future, would force Blue to ship all items to wrong locations. Therefore, all parts will be missing.

Long-term views must consider the short-term metrics and how a combination of those metrics may provide the big picture of what will be the black swan event (Red's long-term objective). Blue must use the tools and metrics provided in this thesis to together with external process, organizational audits, and health assessments to attempt to identify those long-term black swan events. The idealization of a supply chain black swan caused by Red, posed as the premise of this thesis, substantiates the notion that short-term cyber-attacks can indeed be considered as precursors for long-term problems.

Further areas of study include the application of the ideas presented in this study to develop a strategy to increase black swan awareness for network supply chains. A study of the cyber-attack scenarios for operational supply chains is recommended.

APPENDIX. OTHER SHORT-TERM VULNERABILITY MANAGEMENT FRAMEWORKS AND INITIATIVES

The following are current initiatives dealing with the cybersecurity threat and are derived in support of Executive Order 13636 (2013). These initiatives help validate how federal and private entities are addressing the cybersecurity threat as it relates to the vulnerability analysis presented in the previous section. Although the list provided is not exhaustive, these initiatives were chosen because of their relevancy to this study. These include federal, both civilian and DOD, as well as commercial frameworks and initiatives to support the president's cyber initiative.

A. DEPARTMENT OF DEFENSE AND OTHER INITIATIVES

1. Department of Defense Initiative

As promulgated by the DOD's FY 2016 Chief Information Officer, the top information-technology priorities include modernizing networks, sharing with mission partners, reducing DOD information-technology costs, defending against cyber-attacks, managing DOD data, empowering mobile data access, and maximizing spectrum of access (DOD 2016). This document is the overarching strategy that enables the needed changes in the DOD's cybersecurity, as required by Executive Order 13636 3 C.F.R.

2. United States Computer Emergency Readiness Team

The goal of the United States Computer Emergency Readiness Team (US-CERT), under the Department of Homeland Security, is to provide the means to share cyber threat vulnerabilities and manage cyber risk (United States Computer Emergency Readiness Team [US-CERT] 2016). US-CERT (2016) recommends this be accomplished by establishing an Internet operations center (https://www.us-cert.gov) that is open 24 hours a day, seven days a week, and responds to incidents, provides technical assistance, and posts recent vulnerabilities.

3. Supply Chain Risk Management Practices for Federal Information Systems and Organizations (NIST SP 800–161)

The National Institute of Standards and Technology (NIST 2015) in Supply Chain Risk Management Practices for Federal Information Systems and Organizations (NIST SP 800–161), has provided guidance to federal agencies for "identifying, assessing, selecting and implementing risk management process and mitigating controls" (2). This document addresses the risks in the supply chain by enumerating the threats and vulnerabilities and by analyzing the likelihoods of these threats exploiting the vulnerabilities and, hence, determining the degree of harm (NIST 2015).

4. Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life-Cycle Approach (NIST SP 800–37)

The purpose of the Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life-Cycle Approach (NIST SP 800–37) is to provide procedures for applying risk management to cyber systems (NIST 2010). The instruction applies the principles from the aforementioned NIST SP 800–161.

5. Managing Information Security Risk Organization, Mission, and Information System View (NIST SP 800–39)

The purpose of Managing Information Security Risk (NIST SP 800–39) is to establish minimum required guidelines to address the management of information systems and their environment (NIST 2011). The author of this publication used tiers of risk management to address risk at all levels. NIST (2011) defines the tiers as organization, mission process, and information-system level and employs a feedback loop to pursue continuous improvement. This was accomplished by framing, assessing, responding, and monitoring risk in ways similar to the seven-step approach by Zsidisin and Richie (2008) and DOD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs (DASD[SE]) 2015). Unfortunately, analysis falls short when assessment of the risk is limited to organizational response and does not account for long-term objectives.

6. Cybersecurity Instruction for the DOD (DODI 8500.01)

The Department of Defense (2014a) published guidance in DOD Instruction (DODI) 8500.01, entitled Cybersecurity, to establish a program to defend and protect the department's information and information technology. This instruction charges the DOD with "implement[ing] a multi-layered cybersecurity risk management" (DOD 2014a, 2). This is accomplished by considering the threats to information systems, making an assignment to a service component's cybersecurity program, addressing risks as early as possible in the system's life-cycle, and making documentation intra-available to promote exchange of similar information between entities (2014a). This document reiterates the importance of having resilient systems that are integrated and interoperable.

DODI 8500.01 uses the same tiers of risk management illustrated in the aforementioned NIST (2011) special publication Managing Information Security Risk, Organization, Mission, and Information System View (NIST SP 800–39). NIST SP 800–39 has precedence.

7. Risk Management Framework for DOD Information Technology (DODI 8510.01)

The Risk Management Framework for DOD Information Technology, DODI 8510.01, applies to the entire DOD with the intention of establishing "an integrated enterprise-wide structure for cybersecurity risk management" by implementing NIST SP 800–39 (DOD 2014b, 2). The instruction accomplishes this by identifying, implementing, assessing, and managing cybersecurity capabilities in six steps. The six steps comprise categorizing, selecting, implementing, assessing, authorizing, and monitoring (DOD 2014b). This process parallels the system life-cycle with risk-management framework activities.

The main disadvantage of this approach is that step one, categorizing, bounds the problem to what the information owner identifies as impacting confidentiality, integrity, and availability. Although enumerating the risks this early in the process is better than no plan at all, bounding the problem too early may limit the discovery of possible threats.

This methodology does not account for long-term views external to the system being analyzed.

8. Microsoft's White Papers

Two white papers by Microsoft Corporation, *Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust* (2011) and *Toward a Trusted Supply Chain: A Risk Based Approach to Managing Software Integrity* (2014) offer a commercial-sector perspective on supply chain risk and its relationship to information and communication systems. The white papers conform to International Organization for Standardization (ISO) 31000 (risk management principles and guidance), a programmatic risk-management process accomplished by conducting risk identification, analysis, and evaluation (Microsoft 2014). ISO 31000 accomplishes this by having a business model perform risk assessment in six phases: planning, discovery, assessment, development, validation, and implementation. During the planning phase, the objectives, scope, and approach of the assessment are defined (Microsoft 2014).

The discovery phase identifies broad classes of threats to software integrity and attempts to recognize the detailed control activities. The white papers by Microsoft (2011; 2014) also state that during assessment and development, the company identifies and documents control categories related to the threats found during discovery. In the subsequent step, the control requirements are met based on a particular group of discovered threats. The result is proposed software integrity policies and procedures, leading to the last phase implementation (Microsoft 2014).

B. CYBER SUPPLY CHAIN VULNERABILITIES

This section explains some of the factors that can be considered vulnerabilities in the cyber supply chain.

1. Malicious Insertion to Software and Hardware

Malicious code can be inserted at any time during the software's life-cycle. The problem can expand further through the software's exposure to hardware parts, firmware, other software, and insider threats. One of the biggest problems in developing today’s computerized and network systems is determining vulnerability aspects of the hardware parts affected—the answers to who, what, where, when, and how. This problem becomes even more complex when, for example, one country assembles a computer whose parts come from multiple countries. Software and firmware, hereafter referred to as software, may also be susceptible to this problem.

2. Contractual Agreements and Hiring Policies

Most if not all of the software and hardware delivered to program managers are outsourced to contractors. Not all contractors are created equal. Depending on the project’s contract, the project managers do not usually have control of the contractor’s hiring policies. It should be understood that contractors might also be susceptible to one or more of the issues illustrated in the following sections, which add to the complexity of system evaluation and vulnerability assessment.

3. Global Network for Parts and Services

In today’s cost-prohibitive environment, many organizations resort to outsourcing manufactured parts from all over the globe. By doing this, organizations are able to produce more parts and services at lower prices. Unfortunately, a computer system that the program manager thinks was developed by a U.S. contractor and assembled in the United States may have been built with parts manufactured elsewhere. When it comes to the program manager’s assessment of the system’s vulnerabilities, it may become time- and cost-prohibitive to assess the vulnerabilities of all parts and services. In addition, due to the complexity of systems, it is nearly impossible to assess 100 percent of the system before it is distributed.

4. Lines of Code

Most software developed for today’s complex environment and organizational needs may contain millions of lines of code. These lines of code provide a set of instructions to perform designed actions. These actions could turn pumps on or off in an oil or gas pipeline when the system reaches a certain pressure, for example. The more complex a system’s features, the more lines of code are required to perform those functions. When program managers face deadlines, assessing all potential software vulnerabilities present in the code becomes time consuming.

5. Recycled Code

In order to save money and time, some software developers recycle code from internal or external sources. This is a widely used practice, especially when some systems require millions of lines of code. Some of the recycled code is available as subroutines that perform lower-system functions. For example, during the development of code for turning a computer on and starting the operating system, the use of a subroutine may be used to conduct the handshake between the system’s basic input/output system, which loads and starts and loads the operating system. The potential vulnerabilities inherent with this practice are analogous to acquiring hardware parts from multiple sources

6. Different Coding Languages

Not all software is coded in the same language, not all software languages are structured the same way, and not all languages present the same level of vulnerabilities. The program manager has limited resources and expertise to assess the multitude of software coding that a particular system may have.

7. Proprietary Code and Features

Some contractual agreements make it nearly impossible for the program manager to reverse-engineer the software delivered and assess for vulnerabilities. In other words, if an independent coder cannot access and read the lines of software code, the vulnerabilities go unanalyzed. The program manager must be able to understand the vulnerabilities involved with this practice. Although he or she may have transferred the risk to the contractor, the program manager is ultimately responsible to deliver a system on time, within budget, and with the agreed design capabilities. If the system does not operate as intended, the overall system's capability may be affected, thus causing mission failure or degradation.

8. Insertion during the Life-cycle Process

After the software or hardware has been delivered to the program manager and has been tested, assessed, and fielded, the system code will most likely be updated and upgraded during its life-cycle. The upgrades and updates may occur either to enhance functionality or to fix other problems that were not found after the system's delivery. The same rigor must be applied to assess vulnerabilities in the software updates and hardware upgrades as when the system was initially developed.

9. Insider Threat

The program manager must be aware of the possibility of malicious insertion due to insider threats in the form of users or technicians either deliberately or out of ignorance. This can be accomplished by, for example, installing unauthorized software, opening a malicious email, or by introducing vulnerability through an external media plug-in to the system. The user may leave the system vulnerable if clear procedures are not delineated for proper use and maintenance.

10. Compatibility with Other Systems

Most complex systems are interconnected and are integrated as part of a system of systems, and some vulnerability can be introduced through inconsistencies or incompatibility (e.g., out-of-date software) issues between them. For example, system A is integrated with system B, but system B has vulnerability and compatibility issues with newer systems. The performance issues of system B can affect the performance and operation of system A, thus introducing a vulnerability.

C. PROBLEMS DUE TO CYBER THREATS: WHY ARE THEY SO HARD TO FIGHT?

Conventional supply chain vulnerability analysis may not be entirely effective against cyber threat. This is because the cyber threat introduces vulnerabilities that are dynamic, unlimited, and without available data. The following section summarizes why a different approach is needed to understand and mitigate the cyber threat.

1. Dynamic Boundary Conditions

According to Clemente (2011), the cyber problem is resistant to a solution because the infiltrating agents and methods are ever changing; this adds difficulty and complexity.

Cyber-attackers evolve intelligently and quickly, and the complexity and interconnectedness of information systems, as well as the number of vulnerabilities, are evolving at a faster pace. The cyber threats and terrain shift continuously, hence, changing the boundary conditions (Larsen et al. 2014).

2. Unable to Enumerate All Attacks

Conventional supply chain vulnerability analysis requires that attacks be enumerated. Enumeration of all possible attacks not feasible in cyber when resources are limited. A program manager may claim that all possible vulnerabilities due to cyber has been accounted for, but as stated by Larsen et al. (2014), this is impossible as vulnerabilities cannot be mitigated if the details of their existence are unknown. Known vulnerabilities can be documented, monitored, assessed and mitigated.

3. Unable to Assign Likelihoods for Adverse Events

Likelihoods are the probabilistic means of determining whether an event will occur and are usually quantitative (Larsen et al. 2014). Moreover, as the authors indicate, the process of assigning likelihoods requires that risks be enumerated. Unfortunately, data for quantitative analysis is unavailable because of confidentiality agreements or risks that have yet to be identified. As stated by Larsen et al. (2014), if there is not data to be analyzed, it is nearly impossible to assess likelihoods via statistical models or by qualitative means.

Cyber risks are tied to the probability of finding the adverse occurrences that may not be found by statistical or probabilistic models; these risks are under the direct influence of intelligent, persistent, and well-resourced adversaries (Bishop 2003).

LIST OF REFERENCES

American Production and Inventory Control Society. 2016. "APICS: Built on a Foundation of Excellence." APICS. http://www.apics.org/about/overview/history.

Arbaugh, William, William Fithen, and John McHugh. 2002. "Windows of Vulnerability." *IEEE Computer Society* 33(12): 52–59.

Assistant Secretary of Defense for Logistics & Materiel Readiness (ASD[L&MR]). 2016 *Supply Chain Metrics Guide*. Washington, DC: Department of Defense, March 3.

Baldwin, Kristen J. 2014. "DOD Program Protection." Presentation. NDIA Program Protection Summit in McLean, VA, May 20. http://www.acq.osd.mil/se/briefs/2014_05_20_NDIA-PPP-Summit%20-Workshop-Baldwin-Final.pdf.

Bishop, Matt. 2003. *Computer Security: Art and Science.* Boston, MA: Addison-Wesley.

Bowman, Robert. 2013. "Why Cybersecurity Is a Supply-Chain Problem." Supply Chain Brain. http://www.supplychainbrain.com/content/blogs/think-tank/blog/article/why-cybersecurity-is-a-supply-chain-problem/

Childerhouse, P, and D.R. Towill. 2011. "A systems engineering approach to supply chain auditing," *Journal of Manufacturing Technology Management* 22(5): 621—640.

Clemente, Dave. 2011. "International Security: Cyber Security as a Wicked Problem." *The World Today* 67(5): 2.

Council of Supply Chain Management Professionals. 2013. "Supply Chain Management Terms and Glossary." CSCMP. https://cscmp.org/sites/default/files/user_uploads/resources/downloads/glossary-2013.pdf.

Department of Defense. 2014a. *Cybersecurity*. DOD Instruction 8500.01. Washington, DC: Department of Defense, March 14.

———. 2014b. *Risk Management Framework (RMF) for DOD Information Technology (IT).* DOD Instruction 8510.01. Washington, DC: Department of Defense, March 12.

———. 2016. "Top Priorities." DOD. http://DODcio.defense.gov/Home.aspx.

Deputy Secretary of Defense. 2015. *Policy Memorandum (PM) 15–001 – Joint Federated Assurance Center (JFAC) Charter*. Washington, DC: Deputy Secretary of Defense. February 9.

Federal Communications Commission. 2016. "Wire Transfer." FCC. https://www.fcc.gov/licensing-databases/fees/wire-transfer

Garcez, Artur, Luis C. Lamb, Krysia Broda, and Dov M. Gabbay. 2003. "Distributed Knowledge Representation in Neural-Symbolic Learning Systems: A Case Study." In Lecture Notes in FLAIRS Conference Vol: 16, Proceedings of the Sixteenth International Florida Artificial Intelligence Research Society Conference, 271–275, St. Augustine: Florida.

Goetschalckx, Marc. 2011. *Supply Chain Engineering*. New York: Springer

Gordon, Sherry. R. 2008. *Supplier Evaluation and Performance Excellence: A Guide to Meaningful Metrics and Successful Results*. Fort Lauderdale, FL: J. Ross Publishing

House of Representatives Committee on Oversight and Government Reform. 2015. *OPM: Data Breach*. House of Representatives, Washington, DC, Rayburn House Office Building.

Hunter, William Scott. 2012. "Real-Time Supply Chain Predictive Metrics." Technical Paper, Missouri University of Science and Technology.

Hurt, Thomas. 2015. "Department of Defense Joint Federated Assurance Center (JFAC) Update, National Defense Industrial Association (NDIA), 18th Annual NDIA Systems Engineering Conference." Department of Defense. http://www.acq.osd.mil/se/briefs/2015_10_28_NDIA18-DODJFAC-Hurt.pdf

Krebs, Brian. 2014. "Target Hackers Broke in Via HVAC Company." Krebs on Security. http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

Kushner, David. 2013, "The Real Story of Stuxnet." Institute of Electrical and Electronics Engineers. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

Lee, Euchang, Yongtae Park, and Jong Gye Shin. 2009. "Large Engineering Project Risk Management Using a Bayesian Belief Network." Expert Systems with Applications, 36: 5880–5887.

Leiphart, Kristine Lee. 2001. "Creating a Military Supply Chain Management Model." Army Logistics University. http://www.alu.army.mil/alog/issues/JulAug01/MS668.htm

National Institute of Standards and Technology. 2010. *Guide for Applying the Risk Management Framework to Federal Information Systems*. NIST SP 800–37. Gaithersburg, MD: National Institute of Standards and Technology.

———. 2011. *Managing Information Security Risk: Organization, Mission, and Information System View*. NIST SP 800–39. Gaithersburg, MD: National Institute of Standards and Technology.

———. 2015. *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*. NIST SP 800–161. Gaithersburg, MD: National Institute of Standards and Technology.

Microsoft Corporation. 2011. “Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust.” Microsoft Corporation. http://download.microsoft.com/download/3/8/4/384483BA-B7B3-4F2F-9366-E83E4C7562D6/Cyber%20Supply%20Chain%20Risk%20Management%20white%20paper.pdf

———. 2014. “Toward a Trusted Supply Chain: A Risk Based Approach to Managing Software Integrity.” Microsoft Corporation. http://download.microsoft.com/download/9/B/D/9BD9FBFF-A1D9-4DA9-954C-EAE9242C689D/Toward%20a%20Trusted%20Supply%20Chain%20white%20paper.pdf

Naylor, Brian. 2015. “OPM: 21.5 Million Social Security Numbers Stolen From Government Computers.” National Public Radio. http://www.npr.org/sections/thetwo-way/2015/07/09/421502905/opm-21-5-million-social-security-numbers-stolen-from-government-computers

Office of the Deputy Assistant Secretary of Defense for Systems Engineering.2015. *Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs*. Washington, DC: Office of the Deputy Assistant Secretary of Defense for Systems Engineering, June 1. http://www.acq.osd.mil/se/docs/RIO-Guide-Jun2015.pdf

Orlik, Anna, and Laura Veldkamp. 2015. “Understanding Uncertainty Shocks and the Role of Black Swans.” Working paper, National Bureau of Economic Research.

Perez, Hernán. 2013. “Supply chain strategies: Which one hits the mark?” Supply Chain Quarterly. http://www.supplychainquarterly.com/archives/2013/01/

Pistikopoulos, Efstratios N., Michael C. Georgiadis, Vivek Dua, and Lazaros G. Papageorgiou. 2011. *Process Systems Engineering: Supply Chain Optimization, Volume 3*, VCH Verlag: Wiley & Sons. Wiley e-book. http://onlinelibrary.wiley.com/book/10.1002/9783527631247

Scott, Colin, Henriette Lundgren, and Paul Thompson. 2011. *Guide to Supply Chain Management.* Berlin: Springer.

Shackleford, David. 2015. "Combatting Cyber Risks in the Supply Chain." SANS Institute. https://www.sans.org/reading-room/whitepapers/analyst/combatting-cyber-risks-supply-chain-36252

Taleb, Nicholas. 2010. *The Black Swan: Second Edition: The Impact of the Highly Improbable*. New York: Random House.

Teller, Christoph, Herbert Kotzab, and David B. Grant. 2011. "Improving the Execution of Supply Chain Management in Organizations." International Journal Production Economics 140(2): 713–720.

Tsai, Timothy P. 2011. "Supply Chain System Engineering: Framework Transforming Value Chain in Business Domain into Manageable Virtual Enterprise and Participatory Production." Technical paper, Southern Methodist University

Tuncel, Gonca, and Gulgun Alpan. 2010. "Risk Assessment and Management for Supply Chain Networks: A Case Study." Computers in Industry 61(3): 250–259.

Ullman, David, and Richard Ast. 2009. "Decisions Based on Analysis of Alternatives (AoA)." MORS, Phalanx, 44(3): 24.

United States Computer Emergency Readiness Team. 2016. "Overview of Cyber Vulnerabilities." US-CERT. https://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities

Warren, Mathew, and William Hutchinson. 2000. "Cyber Attacks against supply chain management systems: a short note," International Journal of Physical Distribution & Logistics Management, 30(7/8): 710–716.

Taylor, Winslow. 2011. "The Principles of Scientific Management." Guttenberg Project. http://www.gutenberg.org/ebooks/6435

Zsidisin, George A., and Bob Ritchie. 2008. *Supply Chain Risk: A Handbook of Assessment, Management & Performance*. New York: Springer.

Zott, Joseph. (2006). "Attacking Joe's Network," SI4113 Combat Systems Engineering Course, Naval Postgraduate School, Lecture 4, Gary Langford, Instructor.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California